ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57301— 2016/ ISO/TS 14441: 2013

ИНФОРМАТИЗАЦИЯ ЗДОРОВЬЯ

Требования защиты и конфиденциальности систем EHR, используемые при оценке соответствия

(ISO/TS 14441:2013, IDT)

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации» (ЦНИИОИЗ Минздрава) и Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии международного документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава — постоянным представителем ИСО ТС 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2016 г. № 1869-ст

4 Настоящий стандарт идентичен международному документу ISO/TS 14441:2013 «Информатизация здоровья. Требования безопасности и конфиденциальности, используемые при оценке соответствия систем EHR» (ISO/TS 14441:2013 «Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им межгосударственные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

В связи с развитием местных, региональных и национальных информационных структур электронного учета здоровья системы электронных карт пациента используются во многих местах оказания медицинской помощи, которые посещают пациенты [клинические системы пункта обслуживания (point of service, POS)]. Помимо таких учреждений, как больницы, в которых системы, установленные в различных отделениях (например, сестринский пост), как правило, интегрированы в карту отдельного пациента, небольшие системы специального назначения, например электронные медицинские карты (Electronic Health Record, EHR), также используются во врачебных кабинетах и других необщественных учреждениях, например относящихся к здравоохранению населения, в которых сложность систем и местной инфраструктуры поддержки ИТ значительно ниже. Так как страны начинают объединять такие системы медицинского обслуживания с инфоструктурами EHR (или же напрямую обмениваться клиническими данными с другими клиническими системами POS посредством связи «система — система»), безопасность и конфиденциальность этих систем становится гораздо более важной и сложной задачей, чем в случаях, когда системы работают автономно или не связаны с другими системами. Для обеспечения надлежащей реализации требуемых стандартов в этих системах, чтобы они могли безопасно взаимодействовать с инфоструктурами EHR и сохранять конфиденциальность информации о пациентах, многие страны используют программы сертификации и проверки соответствия с целью обеспечения объективного свидетельства соответствия этим требованиям.

Настоящий стандарт определяет требования к безопасности и конфиденциальности, собранные из вышеперечисленных стандартов и основанные на мировом опыте, которые должны быть реализованы на момент аттестационного тестирования совместимых клинических систем POS (электронная карта пациента), взаимодействующих с EHR.

Рассмотренные клинические системы POS принимают, хранят, обрабатывают, отображают и передают клинические данные и действия по управлению, а также информацию, относящуюся к пользователям системы (демографические, персональные данные).

Доступ к системе разрешен только уполномоченным и зарегистрированным пользователям. Такими пользователями являются:

- медицинские работники, которые осуществляют ввод, выбор и используют данные пациента, клинические методики и статистические данные;
- администраторы, которые вносят и читают персональные и демографические данные пациента, административную и статистическую информацию;
- администраторы, которые контролируют полномочия пользователей, создают резервные копии, предоставляют конфигурацию системы, включая тех, которые отвечают за безопасность;
- аудиторы, которые изучают аудиторские следы;
- другие системы EHR, которые вводят и принимают данные;
- объекты получения медицинской помощи и их представители, принимающие решения, имеющие ограниченный доступ к вводу и выбору утвержденных данных.

К совместимым клиническим системам POS применяются следующие основные допущения:

- объект оценки (ТОЕ) может включать в себя коммерчески доступное (COTS), государственное, запатентованное и бесплатное программное обеспечение (ПО), а также ПО с открытым исходным кодом;
- аутентифицированные пользователи признают необходимость в защищенной информационной среде;
- аутентифицированные пользователи могут быть проверены на соответствие политике обеспечения безопасности организации;
- способы обеспечения коммерческой безопасности реализуются с учетом того, что может (и не может) быть выполнено в клинических условиях должным образом;
- надлежащее управление системой защиты выполняется в процессе установки эксплуатации системы.

Настоящий стандарт основан на международных стандартах, которые были разработаны ИСО/ТС 215 для EHR, а также других стандартах ИСО, например, серии стандартов ИСО/МЭК 27001 и ИСО/МЭК 17000, разработанных комитетом ИСО по оценке соответствия (CASCO). Настоящий стандарт также отражает опыт, которым различные страны обладают в настоящее время, в реализации программ сертификации и проверки соответствия для соблюдения требований конфиденциальности

и безопасности в условиях, при которых клинические системы электронных карт пациента в пунктах обслуживания могут иметь возможность работать с региональными и национальными EHR, поддерживая интероперабельность.

Настоящий стандарт включает в себя:

- требования безопасности и конфиденциальности, которые необходимо соблюдать для обеспечения защиты информации, а также основные категории нарушения безопасности;
- обзор теоретической базы требований;
- руководство по передовым практическим методам по составлению и поддержанию программ оценки соответствия;
- описание процесса оценки соответствия, включающее ключевые понятия и технологии.

В приложении А предоставлены более подробная информация о моделях и процессах оценки соответствия, а также примеры программ оценки соответствия в четырех странах (на период 2010 г.).

В приложении В предоставлена детальная проверка требований конфиденциальности и безопасности на месте в пяти юрисдикциях на момент подготовки настоящего стандарта. Данный анализ был использован при определении требований к конфиденциальности и безопасности, приведенных в разделе 5.

Настоящий стандарт должен использоваться агентствами, которые проводят аккредитацию или используют программы для сертификации медицинских программных продуктов посредством оценки соответствия в соответствии со стандартами по конфиденциальности и безопасности, поставщиками программного обеспечения, доказывающими соответствие продукции этим требованиям, и заказчиками данных систем, которым необходима гарантия того, что требования соблюдены.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАТИЗАЦИЯ ЗДОРОВЬЯ

Требования защиты и конфиденциальности систем EHR, используемые при оценке соответствия

Health informatics. Security and privacy requirements of EHR systems for use in conformity assessment

Дата введения — 2018—01—01

1 Область применения

Настоящий стандарт распространяется на системы электронных карт пациента в пунктах медицинского обслуживания, которые обеспечивают взаимодействие с системами EHR. Аппаратные средства и средства управления технологическим процессом не входят в область применения. Настоящий стандарт рассматривает проблемы их безопасности и защиты конфиденциальности путем предоставления ряда требований безопасности и конфиденциальности наряду с руководством и передовыми практическими методами для оценки соответствия.

Стандарт ИСО/МЭК 15408 (все части) определяет «объект оценки» для оценки безопасности продуктов ИТ. Настоящий стандарт включает перекрестное сопоставление 82 требований безопасности и конфиденциальности в соответствии с категориями общих критериев в ИСО/МЭК 15408 (все части). Клиническое программное обеспечение пунктов обслуживания (POS), как правило, является частью большей системы, например, функционирует на основе операционной системы, таким образом, оно должно работать совместно с другими компонентами для обеспечения надлежащего уровня безопасности и конфиденциальности. Несмотря на то что профиль защиты (PP) включает в себя требования к функциям безопасности компонентов для поддержки служб безопасности системы, он не определяет протоколы и стандарты для оценки соответствия и не затрагивает требований конфиденциальности.

Настоящий стандарт сосредоточен на двух основных вопросах:

a) Требования безопасности и конфиденциальности (раздел 5). Раздел 5 является техническим и предоставляет исчерпывающий набор 82 требований, необходимых для защиты (информации, пациентов) от основных видов риска, рассматривает вопросы безопасности и конфиденциальности мест оказания медицинской помощи, совместимых клинических (электронная карта пациента) систем. Данные требования применимы при оценке соответствия.

b) Передовая практика и руководство по созданию и поддержке программ оценки соответствия (раздел 6). Раздел 6 дает общее представления о принципах и методах оценки соответствия, которые могут быть использованы органами государственного управления, организациями местного управления, профессиональными объединениями, разработчиками программного обеспечения, объединениями по медицинской информатике, представителями пациента и другими с целью повышения уровня соответствия требованиям безопасности и конфиденциальности медицинского программного обеспечения. Приложение А предоставляет дополнительную информацию, которая может быть полезна для

Издание официальное

разных стран при проектировании программ оценки соответствия, например дополнительный материал по моделям бизнес-процесса оценки соответствия, методам и другим аспектам, а также наглядные примеры оценки соответствия в четырех странах.

Политика, применяемая к местным, региональным или национальным условиям реализации, а также методическим, административным и физическим (включая аппаратное обеспечение) аспектам управления безопасностью и конфиденциальностью, не входит в область применения данного стандарта. Управление безопасностью входит в область применения ИСО 27799.

2 Нормативные ссылки

Следующие документы полностью или частично приведены в нормативных ссылках в настоящем стандарте, и их применение является необходимым. Для датированных ссылок используются только цитированные издания. Для недатированных ссылок применяется последнее издание документа, приведенного в ссылке (включая любые поправки).

ISO/IEC 17000, Conformity assessment — Vocabulary and general principles (Оценка соответствия. Словарь и общие принципы)

ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002 (Информатизация здоровья. Менеджмент информационной безопасности в здравоохранении по стандарту ИСО/МЭК 27002)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

3.1 **подотчетность** (accountability): Принцип, в соответствии с которым физические лица, организации и общество ответственны за свои действия и могут быть обязаны объяснить их другим.

[ИСО 15489-1:2001, статья 3.2]

Примечание — Требуется, чтобы все пользователи ПМД были доступны прослеживанию.

3.2 **контроль доступа** (access control): средство, благодаря которому доступ к ресурсам системы обработки данных разрешен только авторизованным лицам и осуществляется установленным способом.

[ИСО/МЭК 2382-8:1998, статья 08.04.01]

3.3 **орган по аккредитации** (accreditation body): Авторитетный орган, который проводит аккредитацию.

Примечание — Как правило, орган по аккредитации получает полномочия от правительства.

[ИСО/МЭК 17000:2004, статья 2.6]

3.4 **обезличивание** (anonymization): Процесс, в результате которого удаляется ассоциация между набором идентифицирующих данных и субъектом данных.

[ИСО/TS 25237:2008, статья 3.2]

3.5 **ресурс** (asset): Все, что представляет ценность для организации.

Примечания

1 В контексте безопасности медицинской информации информационные ресурсы включают медицинские данные, IT-сервисы, аппаратные средства, программное обеспечение, средства связи, информационные носители, IT-аппаратуру и медицинские приборы, регистрирующие или сообщающие данные.

2 По ИСО/МЭК 27000:2012, статья 2.4.

3.6 **гарантия** (assurance): Результат набора методов соответствия, с помощью которого организация достигает доверия в статусе управления информационной безопасностью.

3.7 **аттестация** (attestation): Выдача заключения, основанного на проверке, с последующим решением о том, что выполнение указанных требований было доказано.

Примечания

1 Итоговое заявление, указанное в настоящем стандарте как «заявление о соответствии», содержит гарантию того, что все указанные требования были соблюдены. Такая гарантия сама по себе не обеспечивает договорных или других правовых гарантий.

2 См. также область аттестации (scope of attestation).

3 По ИСО/МЭК 17000:2004, статья 5.2.

3.8 **аудит** (audit): Систематический, независимый и документированный процесс получения записей, фиксирования фактов или другой соответствующей информации и их объективной оценки с целью определения степени выполнения указанных требований.

Примечание — В то время как понятие «аудит» относится к системам управления, понятие «оценка» относится к органам по оценке соответствия, а также используется в более общем смысле.

[ИСО/МЭК 17000:2004, статья 4.4]

3.9 **готовность** (availability): Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.

[ИСО/МЭК 27000:2012, статья 2.10]

3.10 **сертификация** (certification): Аттестация, проводимая третьей стороной, относящаяся к продукции, процессам, системам или лицам.

Примечание — По ИСО/МЭК 17000:2004, статья 5.5.

3.11 **соответствие** (compliance): Действие, направленное на то, что необходимо для выполнения установленного требования.

3.12 **конфиденциальность** (confidentiality): Свойство, при котором информация недоступна или закрыта для неавторизованных лиц, субъектов или процессов.

[ИСО 7498-2:1989, статья 3.3.16]

3.13 **оценка соответствия** (conformity assessment): Доказательство того, что заданные требования, относящееся к продукции, процессу, системе, лицу или организации, выполнены.

Примечание — По ИСО/МЭК 17000:2004, статья 2.1.

3.14 **система оценки соответствия** (conformity assessment system): Правила, процедуры и руководство для выполнения оценки соответствия.

Примечание — Системы оценки соответствия могут действовать на международном, региональном, национальном или субнациональном уровне.

[ИСО/МЭК 17000:2004, статья 2.7]

3.15 **субъект данных** (data subject): Лицо, к которому относятся данные.

Примечание — В настоящем стандарте термин «субъект данных» относится к отдельному лицу (в отличие от группы лиц).

3.16 **субъект** (entity): Физическое или юридическое лицо, орган власти, учреждение или любой другой орган.

Примечание — В контексте, не входящем в область применения настоящего стандарта, термин «субъект» может применяться к физическому лицу, животному, организации, активному или пассивному объекту, устройству или группе предметов, которые обладают идентификационными данными.

3.17 **деятельность по оценке соответствия первой стороной** (first-party conformity assessment activity): Деятельность по оценке соответствия, которую осуществляют лицо или организация, представляющие объект.

Примечания

1 См. также деятельность по оценке соответствия второй стороной и деятельность по оценке соответствия третьей стороной.

2 По ИСО/МЭК 17000:2004, статья 2.2.

3.18 **медицинская информационная система** (health information system): Хранилище информации о здоровье субъекта получения медицинской помощи в форме, удобной для обработки вычислительной машиной, надежно хранящейся, передаваемой и доступной нескольким зарегистрированным пользователям.

[ИСО 27799:2008, статья 3.1.2]

Примечания

1 Она имеет общепринятую логическую информационную модель, которая не зависит от систем EHR (электронная медицинская карта).

2 Ее основной целью является поддержка постоянной, эффективной и качественной интегрированной медицинской помощи; она содержит информацию, которая является ретроспективной, одновременно используемой и перспективной.

3.19 **медицинская помощь** (healthcare): Любые виды услуг, оказываемые специалистами или средним медицинским персоналом, влияющие на состояние здоровья.

[Европейский парламент, 1998, согласно ВОЗ]

3.20 **медицинская организация** (health organization): Организация, напрямую участвующая в осуществлении деятельности в области здравоохранения.

Примечание — По ИСО/TR 20514:2005, статья 2.21.

3.21 **специалист здравоохранения** (health professional): Лицо, уполномоченное авторитетным органом на осуществление определенной медицинской деятельности.

Примечания

1 По материалам ИСО 17090-1:2008, статья 3.1.8.

2 Определяемым термином часто является «работник здравоохранения». В настоящем стандарте было принято правило, на основании которого термин «медицинская помощь» (healthcare) сокращается до «медицинский» при использовании в форме прилагательного. При использовании в форме существительного слово «помощь» сохраняется, но в качестве отдельного слова (например, предоставление медицинской помощи).

3.22 **идентичность** (identity): Набор атрибутов, которые позволяют распознать, связаться или обнаружить объект оказания помощи.

3.23 **опознаваемое лицо** (identifiable person): Тот, кто может быть идентифицирован прямо или косвенно, в частности с помощью идентификационного номера или с помощью одного или более факторов, определенных для его физической, физиологической, умственной, экономической, культурной или социальной идентичности.

[Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 г. по вопросам защиты отдельных лиц в области обработки персональных данных и свободного перемещения таких данных]

3.24 **идентификация** (identification): Опознание лица в определенном домене с помощью набора его или ее атрибутов.

3.25 **управление информацией** (information governance): Процессы, с помощью которых организация получает гарантию того, что риски, связанные с ее информацией и, следовательно, с операционными возможностями и целостностью организации, определены и эффективно контролируются.

3.26 **конфиденциальность информации** (information privacy): Права и обязанности отдельных лиц и организаций, связанные со сбором, использованием, хранением, разглашением и удалением личных данных.

[Основано на определении конфиденциальности из «Общепринятых принципов сохранения конфиденциальности» Американского института дипломированных бухгалтеров-ревизоров и дипломированных бухгалтеров Канады]

3.27 **защита информации** (information security): Сохранение конфиденциальности, целостности и доступности информации.

Примечание — Кроме того, могут быть включены другие характеристики, такие как подлинность, подотчетность, воспрепятствование отказу от авторства и достоверность.

[ИСО/МЭК 27000:2012, статья 2.30]

3.28 **проверка** (inspection): Проверка проектирования продукции, процесса или установки и определение их соответствия заданным требованиям или на основе профессионального суждения — общим требованиям.

Примечание — Контроль процесса может включать в себя проверку персонала, оборудования, технологии и методологии.

[ИСО/МЭК 17000:2004, статья 4.3]

3.29 **персональные данные о состоянии здоровья**; ПМД (personal health information; PHI): Информация о распознаваемом лице, которая относится к физическому или психическому здоровью отдельного лица или к оказанию медицинских услуг отдельному лицу.

Примечания

1 Такая информация может включать в себя: a) информацию о регистрации лица для предоставления медицинских услуг; b) информацию о платежах или наличии права на оказание медицинской помощи лицу; c) числа, символы или детали, присвоенные лицу для однозначной идентификации лица в медицинских целях; d) любую

информацию о лице, собранную в ходе предоставления ему медицинских услуг; e) сведения, полученные в ходе выполнения обследования или осмотра части тела или телесного вещества; f) идентификацию личности (например, медицинского работника) как лица, предоставляющего медицинские услуги объекту.

2 Персональные данные о состоянии здоровья не включают информацию, которая является анонимной самостоятельно или в сочетании с другой информацией, доступной для носителя, т. е. отличительные признаки лица, являющегося субъектом информации, не могут быть установлены на основе данной информации.

3.30 **Разглашение ПМД** (PHI disclosure): Разглашение или предоставление доступа к персональным медицинским данным.

Примечание — По материалам ИСО/ТС 25237:2008, статья 3.20.

3.31 **клиническая система пунктов обслуживания**; POS (point-of-service; POS clinical system): Система, которая используется в пунктах оказания медицинской помощи или медицинских услуг объекту оказания помощи.

Пример — Электронная медицинская карта (EMR), Система фармацевтического менеджмента (PMS), Больничная информационная система (HIS), Информационная система общественного здравоохранения (PHIS).

3.32 **нарушение конфиденциальности** (privacy breach): Ситуация, при которой персональные данные о состоянии здоровья были обработаны незаконно или с нарушением одного или нескольких соответствующих правил соблюдения конфиденциальности.

3.33 **управление конфиденциальностью** (privacy control): Технические и организационные меры, направленные на снижение рисков, которые могут привести к нарушению конфиденциальности.

Примечания

1 Средства управления конфиденциальностью включают в себя правила, процедуры, руководящие указания, методы или организационные структуры, которые могут носить административный, технический, контрольно-организационный или правовой характер.

2 Термин «управление» также используется в качестве синонима терминов «мера безопасности» или «контрмера».

3.34 **политика конфиденциальности** (privacy policy): Спецификация целей, правил, обязанностей и средств контроля конфиденциальности применительно к обработке персональных данных о состоянии здоровья в отдельной ситуации.

3.35 **предпочтения конфиденциальности** (privacy preferences): Конкретный или предполагаемый выбор, сделанный лицом касательно того, как должны обрабатываться его/ее персональные данные о состоянии здоровья.

3.36 **принципы конфиденциальности** (privacy principles): Набор общих значений, регулирующих защиту конфиденциальности ПМД при обработке в системах ИКТ.

3.37 **оценка риска для конфиденциальности** (privacy risk assessment): Анализ рисков нарушения конфиденциальности, возникающих в планируемой операции обработки.

Примечание — Данный анализ, также известный как оценка последствий нарушения конфиденциальности, обеспечивается с целью: a) обеспечения соответствия обработки применимым правовым, нормативным требованиям и требованиям политики в отношении конфиденциальности; b) определения рисков и результатов обработки ПМД; c) изучения и оценки средств контроля конфиденциальности и альтернативных процессов обработки ПМД с целью снижения выявленных рисков нарушения конфиденциальности.

3.38 **требования к обеспечению безопасности конфиденциальности** (privacy safeguarding requirements): Критерии, выполнение которых необходимо при реализации средств контроля конфиденциальности, предназначенных для содействия снижению рисков нарушения конфиденциальности.

3.39 **процедура** (procedure): Установленный способ осуществления деятельности или процесса.

[ИСО 9000:2005, статья 3.4.5]

3.40 **обработка ПМД** (processing of PHI): Любые действия или набор действий, выполняемых с ПМД (например, сбор, хранение, управление доступом, анализ, объединение, передача, разглашение или задержка).

3.41 **профиль** (profile): Набор автоматически сгенерированных данных, характеризующих категорию лиц, который предназначен в основном для проведения анализа или прогнозирования персональных предпочтений, поведения и отношений.

3.42 **продукт** (product): Результат процесса.

Примечания

1 Четыре общие категории продукции указаны в ИСО 9000:2005: сервисы (например, транспорт); программное обеспечение (например, компьютерная программа, словарь); техническое обеспечение (например, мотор, механическая деталь); обработанные материалы (например, смазочный материал). Большинство продуктов включают элементы, принадлежащие к различным общим категориям продукта. Продукт называется сервисом, программным обеспечением, техническим обеспечением или обрабатываемым материалом в зависимости от преобладающего элемента.

2 Заключение о соответствии может рассматриваться как продукт аттестации.

3 По ИСО 9000:2005, статья 3.4.2.

3.43 **псевдонимизация** (pseudonymization): Процесс, применяемый к ПМД, который заменяет информацию об идентификационных данных псевдонимом.

Примечание — Перевод в анонимную форму обеспечивает, например, использование ресурса или сервиса объектом получения помощи без раскрытия личности, сохраняя при этом ответственность за такое использование. После перевода в анонимную форму остается возможность определения личности объекта получения помощи на основе псевдонима и/или связи действий объекта друг с другом и впоследствии с объектом получения помощи.

3.44 **проверка** (review): Контроль пригодности, соответствия и эффективности действий выбора и определения, а также результатов этих действий в отношении выполнения установленных требований объектом оценки соответствия.

[ИСО/МЭК 17000:2004, статья 5.1]

3.45 **риск** (risk): Сочетание вероятности события и его последствий.

Примечание — По ИСО 73:2009, статья 1.1.

3.46 **оценка риска** (risk assessment): Целостный процесс анализа и оценки риска.

Примечание — По ИСО 73:2009, статья 3.4.1.

3.47 **управление риском** (risk management): Скоординированные действия по руководству и управлению организацией в области риска.

[Руководство ИСО 73:2009, статья 2.1]

Примечание — Управление риском, как правило, включает в себя оценку риска, обработку риска, принятие риска, информирование о рисках, мониторинг риска и проверку риска.

3.48 **обработка риска** (risk treatment): Процесс выбора и реализации мер по модификации риска.

Примечание — По ИСО 73:2009, статья 3.8.1.

3.49 **отбор образцов** (sampling): Предоставление образцов объекта оценки соответствия согласно процедуре.

[ИСО/МЭК 17000:2004, статья 4.1]

3.50 **область подтверждения соответствия** (scope of attestation): Диапазон или характеристики объектов оценки соответствия, охватываемые подтверждением соответствия.

[ИСО/МЭК 17000:2004, статья 5.3]

3.51 **деятельность по оценке соответствия второй стороной** (second-party conformity assessment activity): Деятельность по оценке соответствия, которую осуществляют лицо или организация, заинтересованные в объекте как пользователи.

Примечание — Лицами или организациями, осуществляющими деятельность по оценке соответствия второй стороной, являются, например, покупатели, пользователи продукции или потенциальные потребители, желающие довериться системе менеджмента поставщика или организации, представляющей их интересы.

[ИСО/МЭК 17000:2004, статья 2.3]

3.52 **установленные требования** (specified requirement): Заявленные потребности или ожидания.

Примечание — Требования могут быть установлены в нормативных документах, таких как регламенты, стандарты и технические условия.

[ИСО/МЭК 17000:2004, статья 3.1]

3.53 **объект получения медицинской помощи, пациент** (subject of care, patient): Одно или несколько лиц, планирующих получить, получающих или получивших медицинские услуги.

Примечание — По ИСО 18308:2011, статья 3.47.

3.54 **целостность системы** (system integrity): Свойство, при котором система выполняет предусмотренные для нее функции без нарушений, преднамеренного или случайного вмешательства, осуществляемого неавторизованным пользователем.

[ИСО 27799:2008, статья 3.2.14]

3.55 **объект оценки** (target of evaluation, TOE): Совокупность программного, программно-аппаратного и/или аппаратного обеспечения, возможно, сопровождаемая руководством.

[ИСО/МЭК 15408-1:2009, статья 3.1.72]

3.56 **проведение испытаний** (testing): Определение одной или более характеристик объекта оценки соответствия согласно процедуре.

Примечание — Термин «проведение испытаний» обычно относится к материалам, продукции или процессам.

[ИСО/МЭК 17000:2004, статья 4.2]

3.57 **деятельность по оценке соответствия третьей стороной** (third-party conformity assessment activity): Деятельность по оценке соответствия, которую осуществляют лицо или орган, независимые от лица или организации, представляющих объект, и от пользователя, заинтересованного в этом объекте.

Примечание — Критерии независимости органов по оценке соответствия и органов по аккредитации представлены в международных стандартах и руководствах, применяемых к их деятельности (см. раздел «Библиография»).

[ИСО/МЭК 17000:2004, статья 2.4]

3.58 **угроза** (threat): Возможная причина нежелательного происшествия, которое может привести к нанесению ущерба системе или организации.

[ИСО/МЭК 27000:2012, статья 2.77]

3.59 **уязвимость** (vulnerability): Неустойчивость ресурса или контроль, который может быть использован угрозой.

4 Сокращения

В настоящем стандарте применяются следующие сокращения:

EHR — электронный учет здоровья;

HL7 — международный стандарт обмена клиническими и административными данными между медицинскими компьютерными приложениями;

ПМД — персональные медицинские данные;

POS — пункт обслуживания;

PP — профиль защиты.

5 Требования безопасности и конфиденциальности

5.1 Общие положения

Данный раздел является техническим и устанавливает ряд требований, описывает меры, необходимые для защиты (информации, пациентов), основные категории риска и широкий ряд вопросов, касающихся безопасности и соблюдения конфиденциальности для пунктов обслуживания, совместимых систем электронных карт пациента.

5.2 Теоретические основы

5.2.1 Общее описание

В связи с ростом внедрения медицинских информационных систем всеми участниками сферы здравоохранения (поставщиками, правительством, плательщиками и пациентами) и необходимостью осуществления обмена информацией о пациенте этими системами с целью повышения стабильности и безопасности медицинского обслуживания пациента существенное значение приобретает обеспечение управления безопасностью электронных медицинских данных для сохранения этими компьютерными системами их целостности, доступности и конфиденциальности.

Переход от традиционных форм хранения амбулаторных карт, основной из которых является хранение на бумажных носителях, к хранению в электронном виде является абсолютно новой формой.

Специалист хорошо понимает риски нарушения безопасности и конфиденциальности, которые, например, возникают при хранении и транспортировке печатных амбулаторных карт. Однако в момент, когда эта информация больше не представлена в печатном виде, а передается в электронной форме и доступ к ней открыт множеству провайдеров во множестве пунктов предоставления услуг, возникает совершенно новая серия рисков. Всем ли пользователям понятно, что риски связаны с хранением и транспортировкой электронных историй болезни? Для того чтобы понять, требуется правильное восприятие всех особенностей вычислительных систем и оборудования, которые обрабатывают информацию, а также новых процессов, которые осуществляются для управления электронной системой.

Цели безопасности включают в себя конфиденциальность, доступность и целостность информации (в данном случае медицинских данных). Отдельные концепции обеспечения безопасности также включены в это широкое определение, такие как достоверность, подотчетность и контролируемость. Последствия нарушения безопасности разнообразны, могут быть как правовыми, так и клиническими, результатом могут являться потеря доступа к информации, необходимой для лечения, и даже серьезные травмы или смерть. С другой стороны, надлежащие средства управления безопасностью позволяют электронным системам работать корректно и поддерживать клиническую деятельность для обеспечения более качественного лечения благодаря наличию достоверной информации в необходимое время и необходимом месте.

Негативное влияние на безопасность и конфиденциальность медицинских данных оказывает множество факторов. При неэлектронном хранении документ может безопасно храниться в запираемых шкафах, однако более важным является то, насколько безопасно хранится ключ от этого шкафа. В то же время в электронной среде существуют электронные компоненты как аппаратного, так и программного обеспечения, которые могут повысить уровень безопасности и конфиденциальности, однако этого недостаточно без сопутствующих процессов, которым должны следовать лица при использовании электронной информации и информационных систем. Высокий уровень безопасности и конфиденциальности является результатом комбинация средств контроля как электронных компонентов, так и процессов. Потеря контроля может привести к нарушению всей защиты.

Примером требования безопасности для программного обеспечения является требование о том, что информационная система должна фиксировать ревизионные сведения по всем операциям, проводимым с амбулаторными картами, включая создание, считывание, обновление и архивацию информации. Примером требования для аппаратного обеспечения является требование о том, что оно должно фиксировать свидетельства повреждений. Примером требования для процесса являются политика и процесс мониторинга, который не позволяет пользователю оставлять пароль видимым и доступным.

Основную ценность представляет информация. Медицинские данные включают:

a) персональную медицинскую и идентификационную информацию;

b) анонимные данные, выведенные из персональных данных о состоянии здоровья посредством методов идентификации с помощью псевдонима;

c) статистические данные и результаты исследований, включая конфиденциальные данные, выведенные из персональных данных о состоянии здоровья путем удаления личных идентификационных данных;

d) клиническая/медицинская информация, не относящаяся к конкретному объекту оказания помощи, включая данные по поддержке принятия клинических решений (например, информация о неблагоприятной реакции на препарат);

e) данные о медицинских работниках, персонале и волонтерах;

f) информация, связанная с надзором в сфере здравоохранения;

g) данные аудиторского следа, выведенные медицинскими информационными системами, которые содержат персональные данные о состоянии здоровья или данные под псевдонимом, взятые из персональных данных о состоянии здоровья, или же содержащие данные о действиях пользователей, связанных с персональными данными о состоянии здоровья;

h) данные системы безопасности для медицинских информационных систем, в том числе данные по управлению доступом и другие данные по конфигурации системы для медицинских информационных систем, связанные с безопасностью.

Из перечня, приведенного выше, важно отметить, что в сфере здравоохранения информация о пациенте является не только конфиденциальной. Степень, в которой конфиденциальность (и, следовательно, конфиденциальность пациента), целостность данных и доступность системы должны быть защищены, зависит от характера информации, области применения, для которой она была внесена, и риска, которому она подвергается. Например, статистические данные могут быть не конфиденциальными,

однако защита их целостности может быть важна для организации. Аналогично данные аудиторского следа могут не требовать высокого уровня доступности, но их содержание может быть строго конфиденциальным.

Область применения настоящего стандарта распространяется на требования безопасности и конфиденциальности для медицинских программных систем. Вопросы, касающиеся аппаратного обеспечения и средств управления процессом, не входят в область применения.

В соответствии с ИСО 27799:2008, приложение А, угрозы нарушения неприкосновенности частной жизни, конфиденциальности, целостности и доступности включают:

a) нелегальное проникновение обслуживающих компаний, внешних лиц, включая хакеров, под видом персонала, например, специалистов и вспомогательного персонала;

b) неразрешенное использование медицинских информационных приложений и данных, хранимых на этих приложениях;

c) появление разрушительного или вредоносного программного обеспечения, включая вирусы, программы-черви и другие вирусные программы;

d) неправильное использование системных ресурсов;

e) несанкционированное проникновение в связь, например, отказ от обслуживания и взлом защиты путем замещения оригинала;

f) перехват информации в каналах связи;

g) отрицание причастности к происхождению или получению данных;

h) нарушение связи;

i) аварийное нарушение маршрутизации;

j) техническую неисправность ведущего компьютера, системы памяти или сетевой инфраструктуры;

k) отказ поддержки жизнеобеспечения, включая перебои электропитания и прерывание обслуживания, вызванное природными или антропогенными катастрофами,

l) отказ прикладного программного обеспечения;

m) ошибку операций,

n) ошибку технического обслуживания;

o) ошибку пользователя.

Несмотря на то что вопросы конфиденциальности медицинских данных широко обсуждаются, существует недостаток системного исследования для определения и классификации различных источников угроз нарушения конфиденциальности информации. Последние исследования, основанные на политике, разделяют угрозы нарушения конфиденциальности на две области:

- организационные угрозы, возникающие в результате несанкционированного доступа к информации о пациенте агентами, превышающими свои полномочия, или внешними агентами, воспользовавшимися уязвимостью информационной системы, и

- системные угрозы, вызванные агентом в цепном потоке информации, использующим данные вне предусмотренной области применения.

Эти два типа угроз описаны в 5.2.2 и 5.2.3.

5.2.2 Организационные угрозы

Эти угрозы принимают различные формы, например, работник, осуществляющий доступ к данным без обоснованной необходимости, или внешний взломщик (хакер), который осуществляет несанкционированный доступ в информационную инфраструктуру организации с целью украсть данные или сделать их неисправными. Широкий спектр организационных угроз можно разделить на пять уровней, перечисленных в порядке увеличения сложности:

- случайное раскрытие информации: медицинские работники непреднамеренно разглашают информацию о пациенте другим (например, отправка электронного письма на неверный адрес или случайное размещение конфиденциальных данных на сайте);

- любопытство членов организации: члены организации, имеющие доступ к данным, проявляют интерес к информации о пациенте из любопытства или для собственных целей (например, получение медсестрами доступа к информации о коллегах по работе для определения наличия заболеваний, передающихся половым путем, или осуществление медицинскими работниками доступа к возможной компрометирующей информации о состоянии здоровья звезд и ее передача средствам массовой информации);

- несанкционированный доступ к данным, осуществляемый членами организации: члены организации осуществляют доступ к информации о пациенте и затем используют, передают или разглашают ее другим с целью извлечения прибыли или из мести;

- несанкционированный доступ к данным посторонних лиц с физическим вмешательством: постороннее лицо осуществляет физическое вторжение путем принуждения или силового доступа внутрь помещения и получает доступ к системе;

- несанкционированный доступ в сетевую систему: постороннее лицо, включая бывших сотрудников, пациентов или хакеров, вторгается в сеть организации извне с целью получения доступа к информации о пациенте или вывода системы из строя.

5.2.3 Системные угрозы

Эти угрозы возникают не за пределами цепочки информационного потока, а от членов организации, которые имеют доступ к информации о пациенте. Например, страховые компании могут отказать в страховании жизни пациента на основе его состояния здоровья или работодатель, имеющий доступ к медицинским картам работников, может отказать в повышении или прекратить трудовые отношения. Пациенты или организации плательщиков могут понести финансовые потери в результате мошенничества, в том числе оказания ненужных медицинских услуг.

5.2.4 Применимость

Как отмечалось ранее, область применения настоящего стандарта ориентирована на безопасность и конфиденциальность программного обеспечения для электронных карт пациента в пунктах обслуживания; аппаратное обеспечение и средства управления процессом не входят в область применения. Существует множество различных требований безопасности и конфиденциальности, разработанных и опубликованных во всем мире, настоящий стандарт не предназначен для создания новых требований, а, скорее, объединяет наиболее подходящие, уже опубликованные требования и адаптирует их для использования при проверке соответствия систем.

Наиболее известным международным стандартом по безопасности является ИСО/МЭК 27002. Несмотря на то что он рассматривает вопросы управления информационной безопасностью в целом, средства управления, описанные в нем, применяются к электронным системам. Стандарт медико-фармацевтической отрасли ИСО 27799 является одним из нескольких стандартов, разработанных в рамках ИСО/ТС 215 для обеспечения реализации программных средств управления и практик в сфере здравоохранения.

В отношении оценки безопасности одним из самых известных стандартов является ИСО/МЭК 15408 (все части). Он устанавливает общие понятия и принципы оценки безопасности информационных технологий и включает в себя общие критерии, через которые могут быть отражены требования безопасности.

В то же время некоторые страны внедряют процессы сертификации медицинских программных систем, каждая со своим собственным набором требований. Некоторые примеры включают США, Канаду, Бразилию, Нидерланды, Великобританию, Австралию и Европу.

Настоящий стандарт определяет требования по безопасности и конфиденциальности, взятые из указанных выше стандартов и международного опыта, которые должны быть согласованы для проверки соответствия совместимых клинических систем POS (электронная карта пациента), взаимодействующих с электронным учетом здоровья.

Набор требований должен быть четко и ясно выраженным. Требования должны быть такими, чтобы разработчики программного обеспечения могли правильно реализовать их в своих системах, а процесс оценки мог подтвердить, что все требования выполнены или не выполнены в этой конкретной системе. Это основная причина, по которой процедурные требования не были включены, так как гарантировать, что они согласованы только с помощью оценки самого программного обеспечения, невозможно: было бы необходимо провести оценку среды, в которой используется эта программа, включая профили пользователей, администраторов и знания в области использования системы. Тем не менее этот более широкий вопрос является необходимым для обеспечения безопасности и конфиденциальности, и поэтому рекомендуется в дополнение к сертификации программного обеспечения и соответствия провести экологическую инспекцию текущего управления системы на основе ИСО 27799. Данное более общее издание, касающееся управления, является необходимым для обеспечения безопасности и конфиденциальности, и поэтому в дополнение к сертификации и проверке соответствия программного обеспечения рекомендуется проводить испытание на воздействие окружающей среды, находящейся под непрерывным управлением системы на основе ИСО 27799.

Другим аспектом в процессе разработки требований является то, что они должны быть настолько устойчивыми к краткосрочным технологическим изменениям и преобразованиям, насколько это возможно. В результате этого ссылки на техническую информацию, например алгоритмы криптограмм,

длина ключа, протоколы и прочее, не были приведены. Справочная информация по этим техническим критериям, может быть необходима.

5.3 Требования конфиденциальности и безопасности POS

5.3.1 Общие положения

В данном разделе представлены требования, которые будут применяться ко всем клиническим системам POS в пределах области применения настоящего стандарта.

5.3.2 Согласие субъекта данных на сбор, использование или раскрытие персональной медицинской информации

Требование 1. Согласие на регистрацию данных. В случае когда субъекты данных имеют право согласно закону или обычаю отказаться или аннулировать свое согласие на использование или разглашение их персональных медицинских данных, клинические системы POS:

a) должны предоставлять средства для регистрации директив согласия субъекта данных, включая отказ или аннулирование согласия;

b) должны иметь возможность выполнить это таким образом, который бы позволил каждой организации соответствовать своим юридическим требованиям или требованиям политики по согласию.

Примечание — Согласие может распространяться на всю персональную медицинскую информацию субъекта данных или на конкретные цели.

Требование 2. Зарегистрировано минимальное количество данных. В случае когда клинические системы POS записывают директивы разглашения информации субъекта данных, должны быть записаны особенности директив (например, отказ от согласия или отказ от согласия, данного ранее), а также тип согласия в тех юрисдикциях, которые распознают два или более типа согласия (например, подразумеваемое или выраженное согласие), и дата, на которую была выдана директива.

Требование 3. Директива, сопровождающая данные. В случае когда субъекты данных имеют право согласно закону или обычаю отказаться или аннулировать свое согласие на сбор, использование или разглашение их персональных медицинских данных, клинические системы POS должны предоставлять средства передачи ограничений на дальнейшее (т. е. последующее) разглашение наряду с разглашаемыми данными, если получатель этих данных не может знать или отвечать директивам согласия субъекта данных иным способом. Клинические системы POS должны иметь возможность выполнения указанного выше таким способом, который позволит отправляющим и получающим юрисдикциям соответствовать собственным законодательным требованиям или политике по согласию.

Требование 4. Экстренный доступ. Срочная медицинская помощь (например, оказание помощи пациенту, находящему без сознания) или другие особые ситуации, допускаемые законом или политикой (например, исследования в области общественного здравоохранения во время эпидемий инфекционных заболеваний), при которых может потребоваться доступ к истории болезни пациента, хранящейся в клинической системе POS, независимо от ранее зарегистрированных директив по разглашению информации. Возможность такого экстренного доступа должна предоставляться только авторизованным пользователям, и его применение (вместе с указанием причины, по которой пользователь игнорирует директиву согласия) должно быть зарегистрировано в журнале аудита. За исключением случаев, когда игнорирование директив согласия допускается законом или политикой, и для того, чтобы устранить неопределенность относительно того, намерен ли пользователь действовать вопреки директиве согласия пациента, система должна разрешить пользователю воспользоваться экстренным доступом напрямую или система должна информировать зарегистрированного пользователя до предоставления доступа о том, что он будет экстренным.

Требование 5. Регистрация экстренного доступа. Клинические системы POS должны быть способны:

a) регистрировать события, при которых обработка директив согласия делает невозможным разглашение данных;

b) регистрировать идентификационные данные любого пользователя, который игнорирует директиву согласия субъекта данных, причину необходимости экстренного доступа, уникальный идентификатор, который будет использоваться позже для идентификации субъекта данных, дату и время использования экстренного доступа;

c) в случаях когда физическое лицо в организации пользователя несет ответственность за содействие соответствию конфиденциальности, информировать об экстренном доступе.

Требование 6. Согласие дано юридически уполномоченным представителем. В случаях когда директива согласия дана от имени объекта получения медицинской помощи юридически уполномоченным представителем, клинические системы POS должны иметь возможность регистрации идентификационных данных этих представителей и степени родства представителя и объекта получения помощи.

Требование 7. Регистрация разрешений на изменения. Клинические системы POS, записывающие разрешающие директивы, должны иметь возможность отображения того, какие разрешающие директивы при их наличии действовали в данный момент времени для данного объекта получения помощи.

Обоснование

Медицинские организации должны знать, что они получили разрешение, требуемое в их юрисдикции, в ходе сбора, использования или разглашения персональных данных о состоянии здоровья. Формы разрешения, необходимые для организации, могут отличаться в зависимости от юрисдикции, обстоятельств, при которых раскрывается информация (например, медицинскому работнику или социальной службе), и типа раскрываемой информации (например, обязательный отчет об инфекционных заболеваниях не требует согласия субъекта данных).

Осуществление ввода персональной медицинской информации в клинические системы POS в рамках конкретной юрисдикции выполняется теми, основным обязательством которых являются получение и регистрация разрешающей директивы субъектов данных, и это часто происходит во время сбора данных, когда получение и регистрация разрешения являются наиболее эффективными. Клиническая система POS должна предоставить средства таким образом, чтобы организация здравоохранения могла гарантировать, что те, кто осуществляет доступ к ПМД, могут получить доступ только к той информации, которая доступна на законном основании либо на основании согласия или законного разрешения (например, если данные раскрываются по распоряжению суда).

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.3 Ограничение использования и разглашения

Требование 8. Регистрация и хранение только тех данных, сбор, использование и разглашение которых имеют определенную цель. Персональная медицинская информация должна использоваться или разглашаться только в целях, совпадающих с теми, для которых она была собрана. Клинические системы POS должны быть структурированы таким образом, чтобы хранение полей данных, не имеющих явного отношения к определенной цели данных, таких как лечение и оказание помощи, выставление счета на медицинские услуги или клинические исследования, не осуществлялось.

Требование 9. Ограничение разглашения информации субъекта данных поставщикам медицинских услуг субъекта данных. Необходима регистрация данного ограничения (например, отказ от согласия или отказ от ранее данного согласия), а также типа согласия в тех юрисдикциях, которые распознают один или несколько типов согласия (например, подразумеваемое или выраженное согласие), и даты, на которую была выдана директива.

Требование 10. Запрет экспорта данных. Передача данных в печатном виде или электронном формате из клинической системы POS в другие системы должна осуществляться только в определенных целях, например, оказание медицинской помощи, резервное копирование данных или передача субъекту данных (или агенту субъекта данных) по запросу субъекта.

Обоснование

Это требование является стандартным и традиционным принципом честного использования данных и не препятствует оказанию помощи поставщиками медицинских услуг. В юрисдикциях, где были введены законодательные акты о защите медицинских данных, эти положения, как правило, разрешают или требуют многократного использования и разглашения персональных медицинских данных, связанных с предоставлением медицинской помощи, поддержкой работы системы здравоохранения или обеспечения общественного здоровья.

Только пользователи клинических систем POS, участвующие в оказании помощи и поддержки объекта, имеют подразумеваемое согласие объекта оказания медицинской помощи на получение доступа к данным субъекта. Без данного согласия нормальный доступ к данным невозможен. Система должна быть обеспечена соответствующим контролем доступа к записям конкретного субъекта данных. Например, доступ к любым медицинским картам пациентов, больше не зарегистрированных в клинике или на приеме, не должен свободно осуществляться пользователями в данной клинике.

Ссылки:

Организация экономического сотрудничества и развития. Принципы честного использования данных (OECD Fair Information Practices).

5.3.4 Доступ субъекта данных к персональной медицинской информации и исправление неточных сведений

Требование 11. Доступ субъекта данных. В случае когда субъект данных оспаривает полноту и точность информации в записи субъекта, а организация не согласна с его оценкой, клиническая система POS должна иметь возможность записи несогласия и/или причины отказа в обновлении записи.

Требование 12. Доступность. Клинические системы POS должны иметь возможность вывода или отображения персональных медицинских данных в формате, подходящем для объекта получения медицинской помощи.

Примечание — В некоторых юрисдикциях субъекты данных имеют право доступа к своим записям и право запроса на внесение изменений в их записи.

Обоснование

Медицинские учреждения, как правило, будут исправлять ошибки только в фактических данных, таких как дата рождения субъекта данных. Вопросы, касающиеся мнения, включая диагноз, поставленный медицинским работником, могут привести к возникновению разногласий по поводу точности медицинской карты. Вопрос, касающийся исправления или дополнения, особенно актуален, если информация может привести к возможным изменениям в лечении пациента или изменениям принятых решений, касающихся его.

Некоторые поправки или дополнения будут иметь особое значение при текущем оказании медицинской помощи субъекту, и эти изменения должны быть соответствующим образом доведены до сведения. К счастью, разработанная система электронного учета здоровья будет иметь возможность автоматически распространять самую последнюю информацию, если это требуется для осуществления официально утвержденных целей.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.5 Точность данных

Требование 13. Точность. Клинические системы POS должны включать средства обеспечения точности и полноты ПМД в той степени, в которой это необходимо для установленных целей применения. Примеры включают в себя внедрение средств контроля проверки ввода данных и осуществление проверок целостности, таких как определение контрольной суммы и хэш-суммы.

Требование 14. Идентификация объекта оказания медицинской помощи. Клинические системы POS должны точно идентифицировать объект оказания медицинской помощи в системе посредством уникальных идентификаторов, допускающих возможность поиска пользователями, при просмотре или изменении карты объекта.

Обоснование

Среда электронного учета здоровья должна способствовать достижению более высокого качества медицинских карт путем встраивания аппаратного контроля на ввод данных и способствования легкому обновлению демографических данных объекта получения медицинской помощи.

Кроме того, точное определение объекта получения медицинской помощи пользователями клинической системы POS до просмотра или изменения их ПМД имеет особое значение для безопасности пациентов.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.6 Идентификация и аутентификация пользователя

Требование 15. Идентификация пользователя. Пользователям клинических систем POS должен быть присвоен идентификатор (ID пользователя), который, возможно, и в комбинациях с другими идентификаторами (например, идентификаторами учреждения или юрисдикции) однозначно идентифицирует каждого отдельного пользователя и используется при аутентификации пользователя и ведении журналов аудита. Если транзакции выходят за пределы организации или юрисдикции, ID пользователя в сочетании с другой регистрационной информацией пользователя (например, имя пользователя, адрес, идентификатор учреждения, идентификатор юрисдикции) должен:

a) однозначно идентифицировать каждого пользователя;

b) позволять принимать решения в системе контроля доступа (см. 5.3.7):

c) позволять сбор результатов аудита (см. 5.3.16), которые могут однозначно связать идентификационную информацию пользователя с проверяемыми действиями пользователя.

Требование 16. Идентификаторы (ID) пользователя. Клинические системы POS должны поддерживать идентификаторы пользователей без учета регистра, которые содержат знаки, взятые из ИСО/МЭК 8859 (все части) [например, ИСО/МЭК 8859-1, также известный как US ASCII (Американский национальный стандартный код для обмена информацией)] или из ИСО/МЭК 10646 [также известный как Unicode (Юникод)].

Требование 17. Аутентификация пользователя. Клинические системы POS должны гарантировать, что все пользователи надежно аутентифицированы.

Требование 18. Аутентификация пользователя. Клинические системы POS должны проводить аутентификацию каждого пользователя перед предоставлением доступа к персональным медицинским данным или соответствующими службами клинических систем POS. По определению, это требование включает доступ, предоставляемый в случаях, когда пользователь не подключен к сети (например, если клиническая система POS доступна для доступа вне сети).

Требование 19. Методы аутентификации. При наличии возможности клинические системы POS должны поддерживать многофакторную аутентификацию пользователя.

Требование 20. Аутентификация пользователя и системы. Клинические системы POS должны аутентифицировать каждое лицо, запрашивающее доступ к ПМД.

Клинические системы POS должны гарантировать подлинность удаленных узлов (взаимная аутентификация узлов) при передаче персональных медицинских данных через Интернет или другие известные открытые сети с помощью защищенного протокола на основе стандартов.

Требование 21. Защита профилей пользователей, паролей и других аутентификационных маркеров. Все данные или параметры, используемые в процессе аутентификации пользователя клинической системы POS, должны храниться или передаваться безопасным способом, обеспечиваться защитой от несанкционированного доступа (в том числе просмотра, изменения или удаления).

При использовании паролей пользователя вместо действующего пароля должны храниться хэш-коды, вычисленные из каждого пароля пользователя, либо пароль должен быть зашифрован с помощью защищенных шифром алгоритмов.

Требование 22. Пароли: использование, качество, сброс и изменения пользователя. При использовании паролей клиническая система POS должна использовать следующие средства контроля безопасности:

a) качество пароля: проверьте качество пароля во время его создания пользователем, убедившись, к примеру, что пароль состоит из как минимум восьми знаков, из которых как минимум один должен быть не буквенным;

b) частота изменения пароля: добавьте функцию, которая требует смены пароля пользователем по истечении настраиваемого максимального интервала времени;

c) смена пароля: предусмотрите административную функцию, которая изменяет пароль. учетные записи пользователя, которые были изменены администратором, требуют пользователя для изменения пароля во время следующей успешной регистрации;

d) чувствительность к регистру: необходима поддержка паролей, чувствительных к регистру, которые содержат знаки, взятые из ИСО/МЭК 8859 (все части) [например, ИСО/МЭК 8859-1, также известный как US ASCII (Американский национальный стандартный код для обмена информацией)] или из ИСО/МЭК 10646 [также известный как Unicode (Юникод)].

Требование 23. Неудачная попытка входа в систему. Клинические системы POS должны принудительно вводить ограничение на последующие неудачные попытки получения доступа пользователем для защиты от дальнейших (возможно, злоумышленных) попыток аутентификации пользователя. Примеры соответствующих механизмов включают блокировку учетной записи/узла до ее отмены администратором, блокировку учетной записи/узла на настраиваемый период времени или задержку следующего приглашения на регистрацию в соответствии с конфигурируемым алгоритмом задержки.

Требование 24. Обратная связь с пользователем в ходе аутентификации. Клинические системы POS должны предоставлять только ограниченный поток обратной информации пользователю в ходе аутентификации, который не содействует пользователю в обнаружении идентификатора пользователя и пароля.

Обоснование

Данное требование облегчает ведение журналов аудита, инициируемых пользователями (например, доступ или изменение записей субъекта данных). Аутентификация также помогает убедиться

в том, что ПМД не скомпрометированы в результате осуществляемого неавторизованными пользователями доступа или изменения.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.7 Управление доступом

Требование 25. Средства управления доступом. Клинические системы POS должны подтверждать, что каждое аутентифицированное лицо или субъект, запрашивающий доступ к персональным медицинским данным, авторизован для допуска к данной информации.

Требование 26. Контроль авторизации. Перед реализацией системы передачи данных, относящихся к ПМД, клинические системы POS должны подтвердить, что запрашивающий пользователь или субъект имеет необходимые права доступа.

Требование 27. Ролевая модель управления доступом. Клинические системы POS должны поддерживать ролевую модель управления доступом (RBAC), имеющую возможность сопоставления каждого пользователя с одной или несколькими ролями и каждой роли с одной или несколькими системными функциями или правами доступа.

Требование 28. Другие формы управления доступом. Клинические системы POS также должны иметь способность сопоставления каждого пользователя с правами доступа, предоставленными или ограниченными на основе:

a) рабочей группы, к которой принадлежит пользователь, или

b) контекста операции (например, время суток, местоположение рабочей станции или экстренный доступ).

Требование 29. Передача доступа к персональным медицинским данным объекта получения помощи. Клинические системы POS должны иметь возможность поддержания ассоциации между выбранными пользователями и картами объекта получения помощи и предоставлять доступ на основе данной ассоциации; т. е. клинические системы POS должны иметь способность предоставления передаваемого доступа к записям на основе передачи пользователем с санкционированным доступом права доступа к этим записям другому пользователю.

При реализации такое предоставление доступа не должно:

a) позволять пользователю с помощью системных средств предоставлять другому пользователю доступ к записям, если предоставляющий пользователь не имеет такого права доступа к записи или

b) превышает основанные на роли права доступа пользователя, получающего доступ.

Требование 30. Сообщение о правах доступа. Клинические системы POS должны иметь возможность сообщения касательно определенного пользователя, имеет ли он доступ к записям определенного объекта получения помощи и разрешения (просмотр, изменение и пр.), касающихся записей объекта получения помощи.

Требование 31. Ограничение прав доступа. В случае если пользователь получает более одной пользовательской роли, то клиническая система POS должна позволить пользователю выбрать ту роль, присвоенную ему, которая применима к необходимому пользовательскому сеансу.

Требование 32. Отмена права доступа. Клинические системы POS должны поддерживать функцию отмены прав доступа пользователя без необходимости удаления пользователя из системы. Клинические системы POS должны исключать пользователей, чьи права доступа для входа в систему были полностью отменены.

Обоснование

В момент, когда система готова к использованию, имеется возможность доступа к ней не только зарегистрированными пользователями, но и, возможно, незарегистрированными. Поэтому системы должны быть разработаны с учетом соответствующих средств контроля доступа. Кроме того, должны предусматриваться элементы управления, которые обнаруживают попытки несанкционированного доступа, а также предпринимают действия для блокировки этих попыток.

На практике пользователи клинических систем POS (их могут быть тысячи) не могут быть индивидуально сопоставлены с функциями системы после их регистрации для контроля их привилегий доступа. Выполнение этого сопоставления для каждого отдельного пользователя является очень сложным и подвержено возникновению множества ошибок. Скорее, пользователи должны быть отображены в роли, а затем роли сопоставлены с функциями системы.

Безосновательно полагать, что все врачи должны иметь возможность получения доступа ко всем записям пациентов в сложной клинической системе POS, так как в ней могут содержаться данные нескольких десятков тысяч субъектов. Необходимо внедрение средств контроля для ограничения доступа

пользователей. Также может существовать необходимость поддержания списка одной или нескольких рабочих групп, членом которой является пользователь. Примеры могут включать хирургические бригады в определенной больнице или врачей с привилегиями доступа в определенной больнице. Такие рабочие группы позволяли бы установление отношений пользователя с субъектом получения помощи на основе существующих отношений между субъектом и другими членами рабочей группы.

Важно отметить, что переданное управление доступом не является управлением, основанным на «ведущей» роли. Например, в допустимых случаях врач общей практики может предоставить другому врачу (к примеру, специалисту) полный доступ к одной из историй болезни своего пациента. Специалист может позже использовать этот допуск для выписки электронного рецепта для пациента. Однако если врач предоставляет доступ медсестре, то медсестра не может позднее выписать электронный рецепт для пациента, так как ролевое управление доступом, как правило, будет предотвращать осуществление такой функции медсестрой.

Требование для отмены права доступа предназначено для обеспечения возможности удаления привилегий пользователя, сохраняя при этом историю пользователя в системе.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789, ИСО/TS 22600 (все части).

5.3.8 Приемлемое использование

Требование 33. Уведомления для пользователей. В каждом сеансе пользователя перед или сразу после входа пользователя в систему или в другой определенный период времени клиническая система POS должна отображать конфигурируемое предупреждение или баннер регистрации, предназначенные напомнить пользователю о конфиденциальности и надлежащем использовании персональных медицинских данных, доступных в системе, и/или применяемых штрафах за неправильное использование системы.

Обоснование

Пользователи клинических систем POS должны быть осведомлены о своих обязательствах (этических и правовых) в отношении персональных медицинских данных, доступ к которым они осуществляют. Несколько юрисдикций реализовали требования, по которым системы отображают на видном месте сообщение сразу после запуска приложения или входа пользователя в систему, информирующее пользователя о его обязательствах и правовых ограничениях, связанных с использованием системы.

Для того чтобы иметь правовую защиту от пользователей, которые проигнорировали средства защиты конфиденциальности информации, осуществив доступ к личной информации, не связанной с их работой, администраторам, возможно, потребуется подтверждение того, что пользователи были четко осведомлены о конфиденциальном характере полученной информации и целях ее использования. Ясное сообщение, выдаваемое после входа пользователя в систему, обеспечивает дополнительную защиту от возможных ложных претензий от пользователей-нарушителей, настаивающих на том, что они не знали о конфиденциальном характере полученной информации или ограничениях ее использования. Ясные предупреждения помогают облегчить процедуру взыскания штрафов с неавторизованных пользователей.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.9 Безопасность сеанса и время ожидания

Требование 34. Безопасность сеанса. Клинические системы POS должны защищать автоматически управляемые рабочие станции от посторонних лиц, пользующихся возможностью использования рабочей станции, пока система функционирует с автоматическим временем ожидания после бездействия.

Требование 35. Время ожидания сеанса пользователя. Клинические системы POS должны защищать автоматически управляемые рабочие станции от проникновения постороннего лица (лиц) с помощью автоматического времени ожидания после настраиваемого периода бездействия пользователя. Примеры такой защиты включают в себя применение программ предохранения экрана или блокировки приложения, требующих повторной аутентификации зарегистрированного пользователя.

Автоматическому времени ожидания должно предшествовать предупреждение (появляющееся в настраиваемый промежуток времени) о том, что время ожидания активируется. Когда время ожидания сессии истекает, этот пользователь должен иметь возможность вернуться к сеансу с помощью повторной аутентификации или другой пользователь должен иметь возможность завершить предыдущий сеанс (без его возобновления) для того, чтобы иметь возможность приступить к новой сессии.

Требование 36. Время ожидания подключения. При необходимости клинические системы POS должны ограничивать продолжительность подключения до интервала времени настройки, чтобы инициировать повторное подключение, если подключение оставалось открытым в течение очень длительного периода времени.

Требование 37. Безопасность сеанса. Клиническая система POS должна иметь средства контроля безопасности сеанса связи для предотвращения похищения или кражи сеанса пользователя.

Обоснование

Многие клинические системы POS уже внедрили защиту сеанса, по крайней мере начального уровня (например, автоматический выход из системы пользователей после периода бездействия или применение режима сохранения экрана, который может быть разблокирован только после повторной аутентификации пользователя). Обратите внимание на то, что поскольку некоторые рабочие станции расположены на физически защищенных участках (например, за счетчиком назначения лекарственных препаратов в аптеках), данное требование может быть неприменимым.

Требование, касающееся времени ожидания подключения, как правило, применяется в безопасных приложениях для инициации повторного подключения (и, следовательно, повторной аутентификации) в случаях, когда подключение осуществлялось в течение очень длительного периода времени. Продолжительность периода поддержания подключения варьируется в зависимости от вида приложения и типа подключения (например, сервер — сервер или клиент — сервер).

Требование, касающееся безопасности сеанса, мотивировано тем, что сеанс может быть украден даже при наличии защиты (например, SSL/TLS). Например, если сеанс отслеживается посредством файла cookie в URL (унифицированный локатор ресурса), то в некоторых ситуациях URL сеанса пользователя может быть получен и использован другим пользователем путем присвоения личности предыдущего пользователя.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.10 Поддержка доступности данных

Требование 38. Резервное копирование. Клиническая система POS должна поддерживать создание резервных копий данных приложения, набора удостоверений защиты, журналов аудита и других данных и файлов, необходимых для нормальной работы клинической системы POS.

Требование 39. Параллельное резервное копирование. Если клиническая система POS доступна в непрерывном режиме, то система должна иметь возможность выполнения параллельного резервного копирования параллельно с работой приложения.

Требование 40. Восстановление. Восстановление данных клинической системы POS должно предоставлять пользователю возможность возврата системы в полностью рабочее и безопасное состояние. Данное состояние должно включать восстановление данных приложения, набора удостоверений защиты и журналов аудита, а также должно обеспечивать возможность проверки полноты восстановленных данных (также см. 5.3.13).

Требование 41. Восстановление содержания электронной карты пациента на предшествующий момент времени. Клинические системы POS должны поддерживать возможность отображения содержания любой карты субъекта данных, которые были записаны или уже имелись на любую предшествующую дату или время.

Обоснование

Клинические данные являются ценным, дорогим, и в ряде случаев незаменимым ресурсом, и их сохранность имеет огромное значение.

Клинические системы POS должны создавать возможность для создания защищенных копий, которые должны соответствовать следующим требованиям:

- экспортируйте атрибуты защиты вместе с данными;
- убедитесь в том, что при восстановлении из резервной копии все атрибуты защиты и их ассоциации были автоматически восстановлены без вмешательства администратора;
- убедитесь в том, что только авторизованный оператор архива мог производить экспорт и восстановление резервной копии, убедившись, что доступ к информации строго ограничен;
- обеспечьте возможность запуска резервного копирования параллельно с работой приложений, для которых система работает непрерывно;
- убедитесь в том, что информация была проверена как при создании, так и при восстановлении ее резервной копии;

- функциональные возможности восстановления системы должны приводить к возврату в полностью рабочее и безопасное состояние, которое включает восстановление данных приложения, набора удостоверений защиты и журналов аудита в их прежнее состояние.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.11 Защита данных в ходе передачи

Клинические системы POS должны применять алгоритмы шифрования информации и протоколы, соответствующие промышленным стандартам, для передачи ПМД по сети Интернет или другим открытым сетям для поддержки конфиденциальности и целостности данных.

Требование 42. Шифрование данных в ходе передачи. В клинической системе, состоящей из компонентов, распределенных по нескольким компьютерам или системам, связь между этими компонентами должна (через Интернет или другие открытые сети) обладать следующими компонентами защиты:

a) аутентификация участника (например, клиента или сервера);

b) целостность данных;

c) конфиденциальность данных.

Примеры

1 Сеансы связи клинической системы POS между компонентом клиента и сервером происходят через Интернет или другие открытые сети с возможностью аутентификации сервера, поддержки целостности данных и конфиденциальности данных.

2 Сеансы связи клинической системы POS между клиентским браузером и Web-сервером происходят через Интернет или другие открытые сети при наличии защиты на основе Web-технологии, например, защиты транспортного уровня (TLS) для обеспечения аутентификации сервера, целостности данных и конфиденциальности данных.

Требование 43. Подтверждение получения данных. С целью гарантии того, что передаваемые данные получены, клинические системы POS должны использовать средства управления безопасностью для подтверждения получения или доставки данных, если передача данных происходит за пределами внешних границ физической защиты, которая обеспечивает безопасность средств обработки информации.

Обоснование

Перехват конфиденциальной персональной информации представляет серьезную угрозу для здравоохранения, и ее злонамеренное изменение при передаче может привести к серьезным последствиям. Обеспечение конфиденциальности и целостности ПМД, передаваемых клинической системой POS, является минимальным требованием.

Юрисдикционные законодательные акты, касающиеся информации о состоянии здоровья, как правило, не содержат конкретных направлений относительно криптографической защиты информации при передаче, однако существует несколько общих требований, которые основаны на отраслевых стандартах по криптографии и криптографическим протоколам.

В случае необходимости, система должна получить подтверждение получения при передаче ПМД, чтобы гарантировать, что передаваемые данные были получены.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.12 Защита данных при хранении

Требование 44. Защита эксплуатационных данных. Клинические системы POS должны следить за тем, чтобы личные данные, журналы аудита и данные, связанные с безопасностью, например профили пользователя, были полностью защищены от несанкционированного доступа и изменения в процессе хранения а базе данных и/или файловых системах.

Требование 45. Защита данных на портативных носителях. При хранении ПМД на любых носителях или съемных и портативных приборах (например, флеш-накопитель, CD-ROM, PDA или портативный компьютер) клинические системы POS должны поддерживать использование формата шифрования, соответствующего отраслевым стандартам.

Требование 46. Защита данных в хранилище данных. Клинические системы, хранящие следующие типы данных, должны обеспечивать защиту этих данных от несанкционированного доступа:

a) персональная информация (например, персональные данные пациента или другая информация, которая идентифицирует пациента);

b) персональные данные о состоянии здоровья;

c) данные системы с особыми требованиями по информационной безопасности (включая данные профилей пользователей и журналы аудита).

Обоснование

Защита ПМД имеет существенное значение, если использование и разглашение данной информации должно контролироваться.

Шифрование хранилищ данных по-прежнему встречается редко в здравоохранении, и медицинские организации не спешат использовать современные технологии для шифрования баз данных. Сотни тысяч незашифрованных карт пациентов были потеряны на портативных носителях с 2007 г. Шифрование играет важную роль для защиты данных на портативных носителях и устройствах.

Защита регистрационных данных пользователя играет важную роль для поддержания их полноты (и, соответственно, целостности процесса аутентификации пользователя). Защита их конфиденциальности также имеет существенное значение для поддержания доверия поставщиков медицинских услуг (которые, к примеру, против неразрешенного разглашения их контактной информации).

Несмотря на то что физическая защита хранилищ данных всегда будет иметь существенное значение (для защиты работоспособности системы), в соответствующих случаях при проектировании новых систем следует рассматривать деидентификацию и шифрование.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.13 Целостность данных

Требование 47. Целостность вводов данных. Данные, импортируемые из других EHR посредством портативного устройства, должны быть четко ассоциированы с объектом получения помощи и лечащим врачом, местом, датой и временем импорта, а также с пользователем, который импортирует данные.

Требование 48. Целостность данных в ходе обработки. Средства управления должны быть готовы к использованию в клинической системе POS для проверки целостности данных EHR с целью предотвращения действий пользователя или отказов системы от несоответствия данных или отказов в целостности ссылочных данных для связей между записями данных.

Требование 49. Целостность выводов данных. Клинические системы POS должны обеспечивать читателю возможность проверки полноты печатных копий документа (например, «страница 3 из 5»).

Обоснование

Эти требования являются минимальными для обеспечения целостности данных. Они также предотвращают плохо защищенное, выборочное отображение данных.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.14 Хранение записей

Требование 50. Хранение. Клинические системы POS должны осуществлять хранение данных в течение периодов, установленных законом или политикой организации. Когда данные больше не нужны, они могут быть удалены, если это разрешено законом и политикой организации. В этом случае они должны быть удалены безопасным способом, стерты или сделаны анонимными таким образом, чтобы процесс удаления не приводил к нарушениям конфиденциальности и безопасности.

Обоснование

Некоторые типы данных объекта получения помощи могут оставаться клинически значимыми в течение многих лет. В нескольких юрисдикциях существуют требования касательно того, что персональные медицинские данные детей или подростков должны оставаться доступными в течение 10 лет после достижения ребенком совершеннолетия (например, восемнадцати лет). Клинические системы POS должны быть построены с учетом таких требований к архивированию, которые позволяют информации храниться до тех пор, пока это необходимо, а впоследствии удаляться безопасным способом.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789, ИСО/TS 21547.

5.3.15 Маркировка данных

Требование 51. Маркировка. Клинические системы POS должны информировать каждого пользователя о конфиденциальном характере и целях использования персональных медицинских данных путем отображения данной маркировки (в согласованном месте и порядке) на печатной

копии, отображающей данные. Клинические системы POS должны либо показывать данную маркировку на любом экране, отображающем данные (в согласованном месте и порядке), либо отображать данную маркировку пользователю при входе в приложение.

Обоснование

Данное требование гарантирует, что все поставщики медицинских услуг и обслуживающий персонал осведомлены о том, что конкретная информация, просматриваемая ими, является конфиденциальной и может быть использована только в конкретных целях (например, лечении и оказании помощи). Это особенно важно в случае, если информация содержится в электронных письмах, факсах и других документах, которые могут содержать конфиденциальную и не конфиденциальную информацию одновременно.

Несмотря на то что известно, что заявления о конфиденциальности могут быть не замечены пользователями, привыкшими к таким предупреждениям, такие заявления остаются преимуществом, обеспечивающим основания для привлечения к уголовной ответственности пользователей, которые не отнеслись к информации с должным вниманием.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.16 Аудит

Требование 52. Регистрация аудита. Клинические системы POS должны регистрировать события, связанные с использованием системы (т. е. запуск и остановка системы, вход и выход пользователя, время ожидания сеанса, резервное копирование и восстановление, блокировка учетных записей) и управлением информацией о состоянии здоровья (т. е. создание, доступ, изменение и архивирование, а также импорт, экспорт, печать или иное разглашение персональных медицинских данных).

Требование 53. Записанная информация. Для каждого из этих событий должна записываться управляющая информация, т. е. время события, идентификация и роль пользователя (в случаях когда пользователь может выбирать одну роль из нескольких перед началом пользовательского сеанса), личность объекта получения помощи и характер события, проверенного аудитом.

Требование 54. Проверка журнала аудита. Файлы журнала аудита должны иметь соответствующие средства защиты для предотвращения изменения и несанкционированного доступа. Примеры таких средств защиты включают средства управления доступом, уникальные порядковые номера для предотвращения удаления, защиту от изменений и периодическое или постоянное резервное копирование.

Требование 55. Интерфейс аудита. Доступ к данным аудита должен строго контролироваться и также подлежать аудиту. Доступ должен осуществляться к соответствующей информационной системе, которая может вводить в действие эти средства контроля, а не непосредственно к самому аудиторскому следу. Система аудита должна предоставлять возможности и инструменты исследования для чтения информации по аудиту из аудиторской документации и запрашивания журнала аудита для:

a) идентификации всех пользователей, которые осуществляли доступ и изменяли определенные записи субъекта данных за определенный период времени, или

b) идентификации всех действий определенного пользователя (включая все доступы к записям субъекта данных) за определенный период времени.

Требование 56. Хранение журнала аудита. Хотя продолжительность хранения файлов журнала аудита является одним из вопросов организационной политики, которая может различаться в зависимости от юрисдикций, система аудита должна поддерживать хранение записей журнала аудита.

Требование 57. События, подвергаемые аудиту. Журналы аудита клинической системы POS должны проверять следующие события:

a) создание, обновление медицинских карт или осуществление доступа к ним (например, отображение на экране, распечатка, скачивание);

b) доступ к данным, которые были защищены или скрыты согласно указанию пациента/лица (экстренный доступ);

c) создание и изменение директив согласия пациента/лица;

d) запрос персональных медицинских данных;

e) импорт ПМД (прием), включая передачу данных, обмен данными;

f) экспорт ПМД, включая передачу данных, обмен данными и печать;

g) действия, связанные с пользователем, ролью и управлением группами, а также

h) доступ к журналу аудита.

Журналы аудита клинической системы POS должны также иметь возможность проведения аудиторской проверки следующих событий:

- запуска и остановки системы;
- попытки аутентификации пользователя и результата (успешно или нет);
- завершения работы пользователя, времени ожидания сеанса, блокировки учетной записи;
- резервного копирования и восстановления (при инициации самой системой);
- доступа к базе данных;
- ошибки аутентификации узла;
- создания/утверждения цифровой подписи;
- событий управления системой защиты, включая изменение пароля, и
- удаления карт.

Клинические системы должны позволять авторизованному администратору устанавливать дополнения и исключения по событиям, подвергаемым аудиту, не включенным в список, указанный выше.

Требование 58. Минимальное содержание записанной информации. Журнал аудита клинической системы POS должен включать следующую информацию:

a) запись с идентификационной информацией пользователя;

b) запись с идентификационной информацией ответственного лица — лица, осуществляющего ввод или доступ к данным, если оно не является пользователем;

c) роль, осуществляемую пользователем (в случаях когда пользователь может выбрать одну из нескольких ролей перед началом сеанса пользователя);

d) организацию пользователя, осуществляющего доступ (в случаях когда пользователь осуществляет доступ к информации от имени нескольких организаций);

e) характер события, подвергнутого аудиту, и идентификатор данных, связанных с событием (например, ID пациента, ID сообщения), подвергнутым аудиту;

f) функции, выполняемые пользователем;

g) временную отметку (дату и время события);

h) в случае экстренного доступа к заблокированным или скрытым записям или частям записей причину экстренного доступа, выбранную пользователем, осуществляющим доступ;

i) идентификационную информацию лица, ответственного за принятие решений, в случае изменений в директивах согласия, внесенных заместителем лица, ответственного за принятие решений;

j) оконечное устройство или точку доступа (при наличии);

k) в случае изменения пароля пользователь, чей пароль был изменен;

l) порядковый номер для защиты от злоумышленных попыток повредить контрольный журнал, например, путем изменения системной даты.

Требование 59. Интерфейс аудита. Клиническая система POS должна поддерживать ведение журнала в общей библиотеке аудита [например, используя схему и средства передачи, указанные в спецификации журнала аудита профиля аудиторских следов и аутентификации узла IHE (ATNA)].

Система должна предоставлять авторизованному администратору возможность считывания информации по аудиту из аудиторской документации по крайней мере одним из следующих способов:

a) система должна предоставлять возможность создания отчетов на основе интервалов дат и времени или

b) система должна иметь возможность экспорта данных журнала таким образом, чтобы обеспечить связь на основе даты и времени [например, синхронизация UTC (всемирное координированное время)].

Требование 60. Защита журналов аудита. Клинические системы POS должны:

a) запрещать пользователям осуществлять доступ к вводимым данным журнала аудита, за исключением тех авторизованных пользователей, которые получили явный доступ с правом считывания информации, и

b) запрещать пользователям вносить изменения в данные журнала аудита.

Система должна защитить доступ к аудиторской документации и должна ограничить доступ к системным инструментам аудита и контрольному журналу, чтобы предотвратить неправильное использование или несанкционированное разглашение частной информации, в том числе удаление или внесение изменений.

Требование 61. Непрерывное ведение журнала. Ведение журналов аудита клинической системы POS должно поддерживаться постоянно, а пользователи не должны иметь никаких средств для отмены любой записи аудита.

Требование 62. Сохранение истории ПМД. Клиническая система не должна стирать записи или данные журнала аудита или вносить изменения в записи субъекта данных, которые препятствуют восстановлению записей объекта получения помощи на предшествующий момент времени.

Обоснование

В области здравоохранения считается, что организации могут определять, кто создал, обновил или осуществлял доступ к записи и когда осуществлялись доступ или изменение. Законным требованием может являться наличие доказательства того, кто создал информацию в медицинской карте. Также распространено требование о том, чтобы работники здравоохранения могли подтвердить необходимость доступа к картам пациентов. В зависимости от законодательства и/или политики юрисдикции может потребоваться официальное разрешение объекта получения помощи. Все вышеуказанное является примером средств управления для обеспечения конфиденциальности пациента и медицинских карт и в то же время поддержания законного использования медицинских карт и их содержания.

Электронные медицинские карты в отличие от карт на бумажных носителях позволяют в большей степени контролировать некоторые из этих аспектов. Автоматизированные средства управления могут применяться для повышения конфиденциальности и обеспечения более высокой поддержки для соответствия законодательным требованиям.

Ведение журнала событий информационных операций и последующих процессов аудита поддерживает подотчетность тех объектов оказания помощи, которые доверили свою информацию системам электронных медицинских карт. Оно также предоставляет мощный стимул пользователям таких систем соответствовать правилам допустимого использования. Эффективное ведение журнала с последующим аудитом доступа к данным и других транзакций может помочь обнаружить ненадлежащее использование систем электронных медицинских карт и данных, а также помочь организациям и объектам оказания помощи получить возмещение от пользователей, злоупотребивших доступом и правами использования данных.

Персональная медицинская информация рассматривается многими как самая конфиденциальная среди всех видов персональной информации, и защита ее конфиденциальности играет важную роль, если необходима поддержка неприкосновенности частной жизни пациента. Для того чтобы защитить целостность персональной медицинской информации, также важно, чтобы весь ее жизненный цикл был полностью защищен и впоследствии подвержен аудиту.

Журналы аудита являются дополнением к реализуемым средствам управления доступом и другими операциями. Журналы аудита предоставляют средства оценки соответствия с политикой управления доступом и могут способствовать улучшению и доработке самой политики. Но так как такая политика должна предвидеть возникновение непредвиденных или чрезвычайных случаев, анализ журналов аудита в этих случаях станет основным средством управления доступом.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.17 Управление версиями программного обеспечения и документация

Требование 63. Управление версиями клинической системы POS. Все компоненты клинической системы POS должны быть идентифицированы и иметь соответствующую версию ПО с отдельной точной ссылкой (уникальный идентификатор, название, поставщик и номер версии).

Требование 64. Документация клинической системы POS. Клинические системы POS должны иметь документацию, которая распространяется на требования и производительность системы, установку и испытание, управление и работу, известные проблемы безопасности, идентификацию и аутентификацию пользователя, права пользования и управление доступом, скрытую связь, аудит, управление изменениями ПО, синхронизацию времени, а также резервное копирование и восстановление.

Требование 65. Изменения документации. Документация должна содержать историю всех изменений для того, чтобы пользователь мог проверить все изменения, внесенные в последнюю доступную версию.

Требование 66. Документация и версии программного обеспечения. Все руководства по эксплуатации должны четко обозначать версию, к которой они применяются, в начале документа.

Требование 67. Версия программного обеспечения. Клинические системы POS должны иметь функцию, которая позволяет пользователю просматривать версию компонентов своего программного обеспечения.

Требование 68. Вопросы, включенные в документацию. Клинические системы POS должны располагать документацией, которая рассматривает следующие вопросы:

a) требования к системе, включая службы и сетевые протоколы, которые необходимы для надлежащего функционирования, а также средства поддержки зависимостей с другими компонентами электронных историй болезни;

b) емкости системных продуктов (например, количество пользователей, количество объектов оказания помощи, количество медицинских карт, сетевая нагрузка) и основные типичные конфигурации, принятые для таких емкостей (например, количество или тип процессоров, конфигурация сервера/рабочей станции и пропускная способность сети);

c) установка, запуск и подключение системы, включая установку защиты связи;

d) этапы, необходимые для подтверждения того, что установка системы была завершена надлежащим образом, а система готова к эксплуатации;

e) управление и работа системы;

f) действия и механизмы обеспечения безопасности, включая создание, изменение и деактивацию учетных записей пользователя; управление ролями, сброс пароля, конфигурирование ограничений пароля и другие аспекты управления правами; защита связи, а также конфигурирование и управление журналами аудита;

g) известные проблемы или конфликты со службами обеспечения безопасности, включая антивирусные программы, уничтожение вредоносных программ, обнаружение проникновения и системы сетевой защиты, а также урегулирование конфликта в применимых случаях;

h) управление изменениями ПО и текущие исправления;

i) синхронизация системного времени (часы) в применимых случаях;

j) сообщения об ошибках системы или работе пользователям и администраторам с указанием необходимых действий;

k) процедуры резервного копирования данных, включая проверку целостности данных при создании или восстановлении резервной копии.

Требование 69. Документация и управление версиями. Все руководства по эксплуатации клинической системы POS должны четко обозначать в начале документа версию, к которой они применяются.

Все обновленные руководства по эксплуатации системы POS должны предоставлять читателю краткое описание изменений последней главной версии.

Требование 70. Изменения в документации. Документация должна содержать историю всех изменений в удобочитаемой форме, чтобы пользователь мог проверить все изменения, внесенные в последнюю доступную версию.

Обоснование

Безопасность зависит от действующих методов и правил организации и проведения работ, а они, в свою очередь, зависят от надежности документации. Управление версиями программного обеспечения также является важным компонентом в управлении безопасностью эксплуатации.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.18 Синхронизация времени и форматирование времени/даты

Требование 71. Формат времени. Клинические системы POS должны принять единый формат отображения времени для осуществления контроля и аудита.

Требование 72. Синхронизация часов. Клинические системы POS должны поддерживать синхронизацию времени с помощью протоколов NTP/SNTP и использовать это синхронизированное время во всех записях безопасности времени.

Требование 73. Формат времени в экспортированных записях. Все данные о времени для осуществления контроля и аудита, найденные в экспортированных данных (за исключением запросов или ответов, поступающих от органа по присвоению временных меток), должны быть представлены в формате ИСО 8601:2004 с указанием разницы между местным временем и всемирным скоординированным временем.

Требование 74. Источники времени. Клинические системы POS должны использовать достоверный и защищенный источник времени.

Клинические системы POS должны поддерживать синхронизацию времени с помощью сетевого протокола синхронизации времени IET (NTP) или простого сетевого протокола синхронизации времени (SNTP).

Обоснование

Точное ведение журнала аудита требует точных и достоверных отметок времени. Кроме того, дата и время, в которое был осуществлен доступ к таким данным, как результаты лабораторных анализов

могут иметь клиническую значимость. Такие временные отметки могут в значительной мере являться официальным доказательством в ходе расследований, связанных с недобросовестной работой медицинского персонала.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789, ИСО 8601.

5.3.19 Контроль инцидентов нарушения безопасности и конфиденциальности

Требование 75. Контроль инцидентов. Клинические системы POS или сопутствующие системы аудита должны отправлять уведомление отдельному лицу организации, ответственному за контроль инцидентов нарушения безопасности или конфиденциальности, каждый раз при обнаружении потенциального инцидента ненадлежащего использования системы (см. также 5.3.2).

Требование 76. Оповещение об инциденте. Клинические системы POS должны предусматривать интерфейс, позволяющий пользователю посылать ответственному лицу уведомление об инцидентах или проблемах безопасности.

Обоснование

Наряду с тем, что решение, кто будет нести ответственность за такие уведомления, является вопросом управления реализовывающей организации, способность клинической системы POS инициировать такие уведомления (например, по электронной почте) может являться высокоэффективным инструментом, быстро устраняющим нарушения конфиденциальности и предотвращающим пропуск инцидентов нарушения безопасности.

Наличие интерфейса в клинической системе POS, позволяющего пользователю посылать ответственному лицу уведомление об инцидентах или проблемах безопасности, может быть полезным.

Примеры ответственных лиц включают сотрудников отдела обеспечения конфиденциальности (далее в некоторых юрисдикциях сотрудники отдела обеспечения конфиденциальности и неприкосновенности частной жизни) и конкретных пользователей с административными полномочиями.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ИСО 27789.

5.3.20 Цифровые сертификаты и электронно-цифровые подписи

Требование 77. Предоставление электронно-цифровых подписей пользователям. Системы POS, располагающие функциями, при которых пользователю необходимо использовать электронный аналог собственноручной подписи, должны предоставлять таким пользователям возможность применения цифровой подписи.

Требование 78. Подтверждение достоверности электронно-цифровой подписи. Каждый раз когда система POS создает и получает данные, содержащие цифровую подпись, при создании и получении система должна подтвердить, что подпись является или являлась действительной на момент ее проставления.

Требование 79. Сохранение электронно-цифровой подписи. Системы POS, позволяющие пользователям применять цифровую подпись или получающие данные, содержащие цифровую подпись, должны хранить, создавать резервную копию или архивировать цифровую подпись каждый раз, когда осуществляется хранение, резервное копирование или архивирование подписанных данных, а также передавать цифровую подпись каждый раз, когда осуществляется передача подписанных данных.

Требование 80. Использование цифровой подписи. Все системы POS, осуществляющие функции, при которых пользователям необходимо использовать электронный аналог собственноручной подписи, должны:

a) позволять пользователям системы применять цифровые подписи с отметкой времени в соответствии с ETSI TS 101 733 (Электронные подписи и инфраструктуры — ESI — CMS. Расширенные электронные подписи — CAdES) или ETSI TS 101 903 (Расширенные электронные подписи XML — XAdES), используя цифровой сертификат с полем для ключа, который обеспечивает отказоустойчивость;

b) на момент подписания проверять, что срок действия сертификата подписавшего не истек, сертификат не аннулирован, а метод сертификации действителен, в соответствии RFC 3280 (Интернет X.509. Инфраструктура открытого ключа. Сертификат и список отозванных сертификатов. Профиль CRL) или RFC 2560 (Интернет X.509. Инфраструктура открытого ключа. Протокол онлайн-получения статуса сертификата — OCSP);

c) позволять всем пользователям системы POS просматривать и подтверждать информацию, которая должны быть подписана в момент подписания.

Требование 81. Проверка подлинности, сохранение и передача цифровых подписей. Система POS должна:

a) по получении подтверждать действительность подписи (т. е. что соответствующий сертификат подписи и вся связанная цепочка сертификатов не были аннулированы),

b) хранить, создавать резервные копии или архивировать цифровые подписи и все связанные с ними данные (информация о корневых сертификатах, цепочки сертификатов, сертификаты подписавшего и информация об аннулировании) всегда, когда осуществляется хранение или архивирование подписанных данных;

c) передавать цифровую подпись вместе с данными или по ссылке каждый раз, когда осуществляется передача подписанных данных;

d) позволять пользователям подтверждать действительность подписи на момент подписания (т. е. что соответствующий сертификат подписи не был аннулирован) каждый раз при осуществлении доступа к подписанным данным.

Требование 82. Цель использования цифровой подписи и роль подписавшего. Системы POS, предоставляющие возможность использования цифровых подписей, должны включать в себя атрибут «индикация типа обязательства» (commitment-type-indication) и роль подписавшего (т. е. атрибут роли подписавшего).

Обоснование

Данное требование действительно для оказания услуг, при которых необходим электронный аналог собственноручной подписи, например, при электронном назначении.

Ссылки:

ИСО 27799, ИСО/МЭК 15408 (все части), ИСО 18308, ETSI TS 101 733, ETSI TS 101 903, RFC3280, RFC2560.

5.4 Общие критерии

Общие критерии (ОК), опубликованные в ИСО/МЭК 15408, состоящем из трех частей, предоставляют общий набор требований к функциям обеспечения безопасности ИТ-продуктов и систем, а также к методам обеспечения достоверности и эффективности, применяемым к этим функциям в ходе оценки защиты.

Стандарт направлен на то, чтобы охватить все различные виды ИТ-продуктов и систем, и предоставляет широкий спектр требований, позволяя разработчику продукта или системы определить область применения, называемую объектом оценки (ОО), и выбрать набор требований, который применяется в конкретном случае.

Так как этот стандарт является международным и общеизвестным, он полезен при отображении связи между требованиями, представленными в настоящем стандарте, и классами ОК. Перекрестное сопоставление, предоставленное ниже, может помочь тем, кто уже знаком с общими критериями, лучше понять настоящий стандарт и наоборот.

Ниже приведен список классов ОК:

a) аудит безопасности (FAU);
b) связь (FCO);
c) криптографическая поддержка (FCS);
d) защита данных пользователя (FDP);
e) (G) идентификация и аутентификация (FIA);
f) (H) управление безопасностью (FMT);
g) (I) неприкосновенность частной жизни (FPR);
h) (J) защита функций безопасности объекта оценки TSF — TOE (FPT);
i) (K) использование ресурсов (FRU);
j) (L) доступ к объекту оценки (FTA);
k) доверенный маршрут/канал (FTP);
l) управление безопасностью:
   - управление версиями;
   - документация и методы;
   - доступность;
   - контроль времени;
m) неприкосновенность частной жизни;
n) защита функций безопасности;
o) управление доступом.

В таблице 1 приведено перекрестное сопоставление классов ОК с требованиями, установленными в предыдущем разделе.

Таблица 1 — Сравнение требований с общими критериями

Требование	Совпадение между требованием и классом ОК	Класс ОК
1 Согласие субъекта данных на сбор, использование и разглашение персональных медицинских данных	—	Нет прямых совпадений для неприкосновенности частной жизни (не рассматривается в ОК)
2 Ограничение использования и разглашения	—	Нет прямых совпадений для неприкосновенности частной жизни (не рассматривается в ОК)
3 Доступ субъекта данных к личной информации и исправление недостоверных сведений	—	Нет прямых совпадений для неприкосновенности частной жизни (не рассматривается в ОК)
4 Достоверность данных	Да	Защита данных пользователя. Целостность хранимых данных
5 Идентификация и аутентификация пользователя	Да	Идентификация и аутентификация
6 Управление доступом	Да	Доступ: политика контроля доступа, функции управления доступом
7 Приемлемое использование	—	Нет прямых совпадений для неприкосновенности частной жизни (не рассматривается в ОК)
8 Безопасность сеанса и время ожидания	Да	Доступ: блокировка и завершение сеанса
9 Поддержка доступности данных	Да	Управление безопасностью
10 Защита данных в ходе передачи	Да	Криптографическая поддержка: работа в режиме криптографической защиты
11 Защита данных при хранении	Да	Защита данных пользователя
12 Целостность данных. Контроль инцидентов нарушения безопасности и конфиденциальности	Да	Защита данных пользователя: целостность хранимых данных
13 Хранение записей	—	Нет прямых совпадений с категориями ОК
14 Маркировка данных	Да	Доступ к объекту оценки
15 Аудит	Да	Аудит безопасности
16 Управление версиями программного обеспечения и документация	Да	Управление безопасностью
17 Синхронизация времени и форматирование времени/даты	Да	Управление безопасностью
18 Контроль инцидентов нарушения безопасности и конфиденциальности	—	Нет прямых совпадений с категориями ОК
19 Цифровые сертификаты и электронно-цифровые подписи	Да	Криптографическая поддержка

6 Современные подходы и руководство по разработке и поддержке программ оценки соответствия

В данном разделе представлен обзор принципов, альтернативных подходов и решений, связанных с разработкой программ оценки соответствия, для гарантии того, что (клинические) системы POS, которые должны быть подключены к инфоструктуре EHR, могут быть проверены на соответствие

различным видам требований безопасности и конфиденциальности, описанным в разделе 5. Данный раздел не содержит требований.

Службы оценки соответствия для медицинского программного обеспечения нужны странам и структурам для выполнения большого количества задач, включая:

- подтверждение покупателю того, что медицинское программное обеспечение соответствует необходимым нормативам;
- защиту здоровья и безопасности объекта получения помощи;
- увеличение возможностей международной торговли;
- обеспечение совместимости и взаимозаменяемости компонентов в пределах комплексных систем и между ними.

Что касается подтверждения того, что требования безопасности и конфиденциальности соблюдены при подключении клинической системы POS к инфоструктуре EHR и/или поддержке связи с другими клиническими системами POS, то программы оценки соответствия или сертификации могут решать каждую из этих задач.

Различные страны использовали разные подходы к своим программам по оценке соответствия в зависимости от своих потребностей, и многие страны разрабатывают, совершенствуют или развивают свои программы для соответствия все более сложным требованиям совместимости. В данном разделе (и материале, представленном в приложении А) используются стандарты ИСО 17000, разработанные Комитетом ИСО по оценке соответствия (CASCO), а принципы этих стандартов применены в контексте здравоохранения, основываясь на опыте четырех стран, который они имели к 2010 г., для того, чтобы проиллюстрировать различные варианты и решения, связанные с разработкой программ оценки соответствия.

Данный раздел находится в сфере интересов правительства, местных органов власти, профессиональных комитетов, разработчиков программного обеспечения, обществ по информатизации здоровья, представителей объектов получения помощи и других лиц, которые заинтересованы в разработке и совершенствовании программ оценки с целью обеспечения соответствия их требованиям совместимости своих EHR.

6.1 Принципы

Оценка соответствия определена Комитетом ИСО по оценке соответствия (CASCO) в ИСО/МЭК 17000:2004 как «подтверждение того, что установленные требования, относящиеся к продукту (включая программное обеспечение), процессу, системе, лицу или органу, соблюдены».

Существуют ключевые компоненты данного определения:

- требуется набор установленных требований, согласно которым будет проводиться оценка соответствия;
- требуются объективные средства подтверждения того, что требования соблюдены;
- требуется привлечение определенного продукта, процесса, системы, лица или органа.

В контексте настоящего стандарта требования безопасности и конфиденциальности установлены выше, в разделе 5. Данный набор требований в дальнейшем может быть ограничен или дополнен странами-участниками и местными органами для решения следующих вопросов:

- вопроса конкретного контекста системы каждой страны-участника в соответствии с определением в объектах оценки и
- вопроса юридических, производственных и технологических потребностей каждого участника, включая требования, содержащиеся в спецификациях поставщиков или покупателей, национальных, региональных или международных стандартах или постановлениях правительства.

А также:

- средства подтверждения того, что требования соблюдены, различаются в зависимости от страны, однако настоящий стандарт предоставляет руководство, основанное на работах комитета CASCO и текущем опыте стран-участников в осуществлении оценки соответствия для внедрения клинических систем POS в инфоструктуры EHR;
- в область применения настоящего стандарта входят только требования по оценке соответствия с учетом того, что различные страны могут иметь дополнительные виды сертификации для процесса и людей, которые разрабатывают, обеспечивают функционирование и реализуют данные продукты в наших комплексных медицинских технологических средах.

Методы подтверждения соответствия включают в себя испытание, осмотр, заявление поставщика о соответствии и сертификацию. На рисунке 1 с помощью наглядной модели выделено отношение между оценкой соответствия и множеством компонентов, которые влияют на его установление:

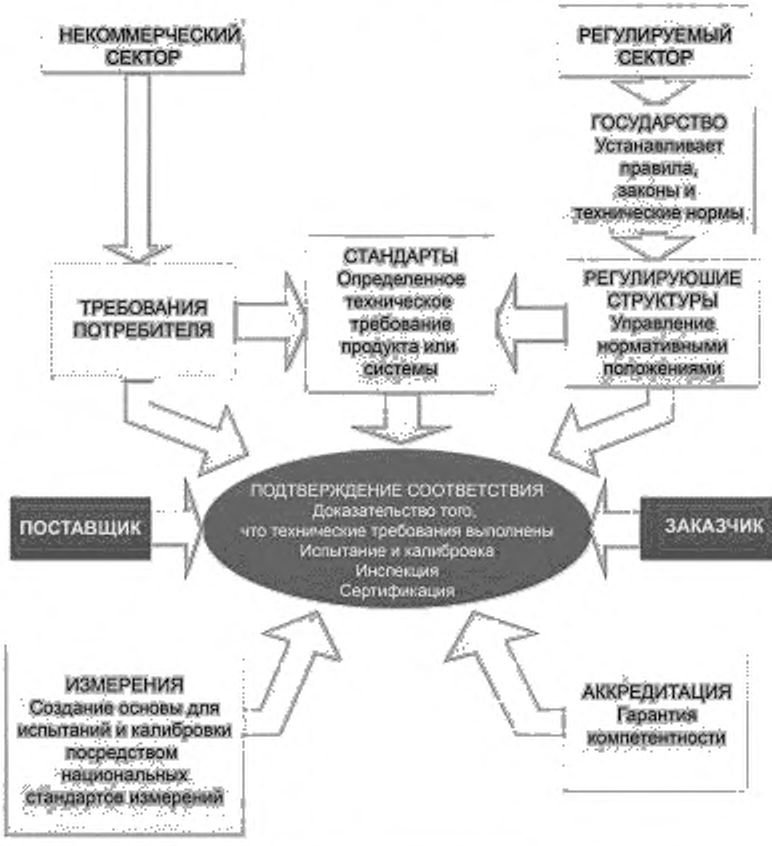

Рисунок 1 — Пример модели оценки соответствия

К данному вопросу относятся три принципа:

- оценка соответствия — подтверждение того, что установленные требования, относящиеся к продукту, процессу, системе, лицу или органу, соблюдены;

- сертификация — аттестация, проводимая третьей стороной, относящаяся к продукции, процессам, системам или лицам;

- соответствие — действие, направленное на то, что необходимо для выполнения установленного требования.

Одной из особенностей оценки соответствия является то, что она может принимать различные формы, используя различные методы в зависимости от задач, для которых она используется. Независимо от того, кем будет проводиться работа — поставщиком продукции, покупателем или независимым органом, требуется четкое понимание необходимости наличия знаний, навыков и опыта у тех, кто выполняет задачи по оценке соответствия. Каждая организация независимо от ее роли должна использовать систему управления, в которой установлены необходимые компетенции и средства подтверждения того, что отдельные лица соответствуют указанным требованиям. ИСО/МЭК 17065 содержит общие критерии для организаций, использующих системы сертификации продуктов; хотя стандарт касается сертификации продукта, проводимой третьей стороной, многие из его положений могут также быть полезными при оценке соответствия продукции, проводимой первой и второй стороной.

Очень часто термин «оценка соответствия» означает только «сертификацию». На самом деле оценка соответствия может быть проведена многими людьми, в том числе поставщиком продукта или услуги, его покупателем и другими заинтересованными сторонами, например, страховыми компаниями и органами регулирования. Это удобно, когда речь идет об оценке соответствия для обозначения сторон следующим образом.

- первая сторона: лицо или организация, которая предоставляет объект, подлежащий оценке соответствия;
- вторая сторона: лицо или организация, которая заинтересована в объекте как пользователь;
- третья сторона: лицо или организация, независящая от лица или организации, предоставляющей объект и заинтересованной в объекте как пользователь.

6.2 Процессы оценки соответствия

ИСО/МЭК 17000 устанавливает «функциональный подход» к оценке соответствия. Функциональный подход включает в себя основные процессы, такие как выбор, определение, рассмотрение и аттестация, а также наблюдение при необходимости.

Каждый этап включает в себя действия, описанные ниже, при этом выход из одного этапа будет являться входом во второй этап.

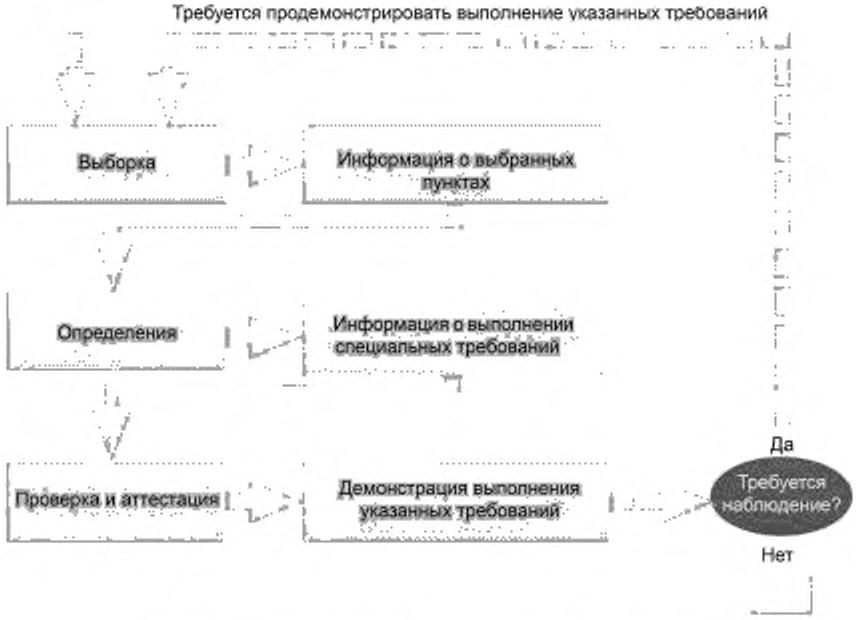

Рисунок 2 — Функциональный подход к оценке соответствия[1)]

Действия, осуществляемые на каждом этапе, могут включать в себя:

Выбор

- Спецификация стандарта (стандартов) или другого документа (документов), соответствие которым будет оцениваться.
- Выбор примеров объектов, которые подлежат оценке.
- Спецификация методов статистической выборки в соответствующих случаях.

Определение

- Тестирование для определения указанных характеристик объекта оценки.
- Проверка физических свойств объекта оценки.

[1)] Рисунок, обозначенный как рисунок 4 в документе ИСО «Построение доверительных отношений. Набор средств по оценке соответствия», Центральный секретариат ИСО, февраль 2010 г.

- Аудит систем и записей, относящихся к объекту оценки.
- Определение качеств объекта оценки.
- Изучение спецификаций и чертежей для проверки и аттестации объекта оценки.

Проверка и аттестация

- Рассмотрение доказательств, собранных на стадии определения, касающихся соответствия объекта установленным требованиям.
- Возвращение к этапу определения для устранения несоответствий.
- Составление и выдача заключения о соответствии.
- Размещение знака соответствия на продукции, соответствующей требованиям осмотра.

Надзор

- Выполнение действий по определению в месте производства или в канале поставок на место торговли.
- Выполнение действий по определению в месте торговли.
- Выполнение действий по определению на месте использования.
- Рассмотрение результатов действий этапа определения.
- Возвращение к этапу определения для устранения несоответствий.
- Составление и выдача подтверждения о сохранении соответствия.
- Выполнение корректирующих и предупреждающих действий в случае выявления несоответствия.

Приложение А дает более детальное описание данных методов, описывая решения, связанные с выбором методов и предоставлением наглядных примеров подходов к оценке соответствия, которые использовали страны-участники.

В случаях когда риски несоответствия высоки (например, общественная безопасность находится под угрозой), как правило, требуется независимый орган для выполнения некоторых определенных видов деятельности по оценке соответствия, по крайней мере для рассмотрения доказательств соответствия и выдачи документа об аттестации, например, сертификата. Данные органы, как правило, взимают плату за свои услуги, а для завершения своей работы им требуется время.

Основным структурным элементом программ соответствия является схема оценки соответствия, которая относится к определенной группе объектов, имеющих достаточно схожие характеристики, которые предоставляют возможность применения того же набора правил и процедур с той же системой управления для оценки соответствия с тем же набором указанных требований.

Владельцу схемы нужно указать, должна ли работа быть проведена одним конкретным органом или любым органом, который отвечает требованиям схемы. В случаях если указана оценка соответствия третьей стороной, следует учитывать необходимость аккредитации таких органов по оценке соответствия.

Несколько стран (например, США, Великобритания, Бразилия и Канада) внедрили программы по оценке соответствия при поддержке национального правительства для расширяемого массива клинических программных продуктов и требований, так как клиническая функциональность и совместимость клинических систем POS увеличивается. Эти программы продолжают развиваться на основе опыта и изменении потребностей, а приложение А представляет собой описание подходов, примененных в четырех странах к 2010 г. В последнее время также появляются подходы, разработанные с участием многих стран, например, проект «Интеллектуальное открытое обслуживание европейских пациентов» [European Patients Smart Open Services (epSOS)].

В случае с США Бюро национальных координаторов (ONC) аккредитовало агентства третьих сторон на право выдачи сертификатов согласно требованиям соответствия и методам проведения испытаний, установленным Национальным институтом науки и техники (NIST). В других странах сертификаты предоставляются отдельным органам, назначенным правительством страны.

Следует отметить, что другие модели оценки соответствия, такие как IHE, несмотря на то что не являются программами по сертификации или их частью, предоставляют производителям программного обеспечения методы для утверждения соответствия и могут использоваться, например, в национальной программе сертификации.

Часто использование знака соответствия контролируется с помощью лицензии, выданной владельцем знака или организацией, действовавшей от имени владельца, например, органом по сертификации. В лицензии излагаются условия, при которых лицензиат может использовать знак, например, ограничения, касающиеся использования его только на тех продуктах, которые поставщик проверил

на соответствие сертифицированному типу продукта. Определение политики использования знаков соответствия является существенно важным для владельца и лицензирующего органа, так как продукция с их знаком часто производится в соответствии с системой, в которой лицензирующий орган проводит проверку только случайных образцов продукта.

Каждая программа по оценке соответствия в США, Великобритании, Бразилии и Канаде включает в себя процесс выдачи сертификационных знаков и публикации перечня медицинских программных продуктов, которые прошли испытания по оценке соответствия, установленные для определенного ряда требований. Такие сертификаты существуют как для целых систем, так и в некоторых случаях для ограниченного числа модулей этих систем.

Приложение А
(справочное)

Программы по оценке соответствия. Конструктивные решения и наглядные примеры от стран-участников на 2010 г.

А.1 Общие сведения

Данное приложение предоставляет более подробную информацию о моделях оценки соответствия, процессах и других решениях, сопровождаемую примерами программ оценки соответствия и сертификации с целью продемонстрировать альтернативные подходы, которые могут быть применены в зависимости от ситуации в определенной стране. Несмотря на то что примеры, приведенные в данном приложении, допускают обмен информацией в пределах государственных границ, их принципы все еще применимы в ситуациях с межгосударственным обменом. Такие проекты, как epSOS [European Patients Smart Open Services (Интеллектуальное открытое обслуживание европейских пациентов)], в Европе являются реальным примером межгосударственного обмена в рассматриваемой области.

А.2 Программы по оценке соответствия. Конструктивные решения

А.2.1 Уполномоченный орган

Методы оценки соответствия могут использоваться первой, второй или третьей стороной: поставщик является первой стороной, покупатель является второй стороной, а организация, не имеющая коммерческой заинтересованности в сделке, является третьей стороной. Решение о том, какая сторона должна реализовывать эти методы, будет зависеть от местных условий. Как указано в 6.2 и проиллюстрировано в четырех программах, описанных далее в данном приложении, модель оценки третьей стороной, включающая государственную сертификацию, принимается часто, поскольку риски нарушения общественной безопасности, вызванные несоответствием клинической системы POS, считаются высокими. Тем не менее при отсутствии государственной программы сертификации местные организаций здравоохранения могут, например, утвердить процесс оценки соответствия второй стороной, чтобы снизить риски внедрения несовместимой клинической системы POS в местную инфоструктуру EHR.

Система оценки соответствия использует общий набор правил, процедур и методик управления для ряда схем оценки соответствия. Для различных схем, возможно, потребуется более подробное описание правил и процедур, различными способами, однако с точки зрения эффективности и стабильности работа в рамках общей структуры является преимуществом.

Каждая схема оценки соответствия будет иметь владельца. Может применяться множество различных методов, некоторыми примерами которых являются:

a) Поставщик программного обеспечения может установить схему оценки соответствия для своих продуктов, включая тестирование, проверку и аудит, с последующей выдачей заявления о соответствии.

b) Схема может быть разработана органом по сертификации для единоличного использования его клиентами, в этом случае орган по сертификации несет полную ответственность за проектирование, применение, управление и обслуживание схемы. Орган будет являться владельцем схемы.

c) Такая организация, как национальное правительство, регулирующий орган или торговая ассоциация, может разработать схему и предложить ее использование одному или нескольким органам сертификации. В этом случае организация будет являться владельцем схемы и нести ответственность за ее работу, возможно, по контракту или другому официальному соглашению с органами сертификации.

d) Группа органов по сертификации, возможно в разных странах, может совместно установить схему сертификации. В этом случае органам как совладельцам схемы будет необходимо создать структуру управления для того, чтобы схема могла эффективно использоваться всеми участвующими органами.

А.2.2 Требования к органам сертификации продукта

Требования к органам, осуществляющим сертификацию продукта, процесса или услуг, определены в ИСО/МЭК 17065.

Основной целью ИСО/МЭК 17065 является определение требований, которым должен соответствовать орган сертификации продукта, процесса или услуг, для подтверждения его компетентности и беспристрастности. Требования структурированы для изучения следующих аспектов управления и работы сертифицирующих органов.

- *Общие требования*: вопросы права и заключения договоров; беспристрастность управления; ответственность и финансирование; недискриминационные условия; конфиденциальность, общедоступная информация.
- *Требования к структуре*: организационная структура и высшее руководство; механизмы сохранения беспристрастности.

- *Требование к ресурсам*: персонал органа сертификации; ресурсы для оценки.

- *Требования к процессу*: схемы сертификации; применение; проверка применения; оценка; рассмотрение; решение сертификации; сертификационная документация; каталог сертифицируемой продукции; надзор; изменения, влияющие на сертификацию; завершение, уменьшение, приостановка или отмена сертификации; записи; жалобы и претенции.

- *Требования к системе управления*: опции; документация на систему управления; контроль организации документов; управление записями; проверка системы управления; внутренний аудит; корректирующие действия, предупреждающие действия.

А.2.3 Вопросы стоимости и другие решения

При принятии решения по соответствующим вопросам организации оценки соответствия для конкретных ситуаций должны рассматриваться затраты на использование альтернативных подходов. Наряду с затратами, понесенными в результате проведения самостоятельной оценки, необходимо учитывать, какие дополнительные расходы могут быть понесены и кем, как только другая сторона начинает принимать участие. Если покупатель продукта решает провести собственную оценку, он, как правило, должен нести расходы, связанные с наймом своих собственных инспекторов.

Если независимый орган заключает контракт на проведение оценки соответствия, ему будет необходимо покрыть свои расходы за счет того, с кем он работает. В случае проведения сертификации продукции, как правило, поставщик будет нанимать орган сертификации и оплачивать его услуги. Расходы органа связаны не только с экспертами, участвующими в оценке, но и со всеми затратами, понесенными в результате осуществления его деятельности, доля которых будет взиматься с каждого заказчика сертификации.

Таким образом, решение о создании схемы сертификации может привести к дополнительным расходам, связанным с поставкой сертифицированной продукции. Аналогичным образом решение о необходимости аккредитации органов по сертификации приведет к дополнительным расходам, так как затраты, понесенные в результате работы органа по аккредитации, также должны быть возмещены.

В дополнение к прямым затратам на оценку соответствия существуют и другие факторы, которые приводят к финансовым последствиям, особенно для поставщиков сертифицированной продукции. Привлечение третьей стороны может привести к задержкам в производстве и поставке продукции в зависимости от интервала между заявкой на сертификацию и получением сертификата соответствия.

А.2.4 Ответственность

Одним из основных принципов оценки соответствия является то, что организация, которая является владельцем объекта оценки или выводит его на рынок, несет основную ответственность за его соответствие установленным требованиям. Поставщик продукта несет договорные и правовые обязанности перед пользователем, которые заключаются в том, что продукт будет выполнять свои заявленные функции и что он не будет ставить под угрозу здоровье или безопасность пользователя или других лиц. Даже если поставщик получает от независимого органа сертификат, подтверждающий то, что продукт соответствует необходимым спецификациям, в случае возникновения проблем он остается ответственным. Несмотря на то что независимый орган может нести некоторую степень ответственности, особенно за небрежное выполнение оценки соответствия, это не освобождает поставщика от основной ответственности. Конечно, ненадлежащее использование продукта конечным пользователем, в частности ненадлежащее выполнение технического обслуживания, может освободить поставщика от ответственности за последующий ущерб и его последствия.

А.2.5 Разработка программы оценки соответствия

Структура программы оценки соответствия должна четко определять объект оценки соответствия, в том числе необходимость отбора проб или образцов, которые будут использоваться в процессе определения. Отбор может также включать в себя выбор наиболее подходящих процедур (например, методы проведения испытаний или методы контроля), которые будут использоваться в процессе определения. Довольно часто бывают случаи, когда должны быть разработаны новые или измененные методы для выполнения действий этапа определения. Необходимо выбрать соответствующие места, условия и частных лиц для выполнения процедуры (процедур). В конечном итоге может быть необходима дополнительная информация для того, чтобы выполнить действия этапа определения для того, чтобы подтвердить, что выполненные установленные требования будут эффективными. Например, объем испытаний, на который должна распространяться аккредитация лаборатории, должен быть определен до выполнения соответствующих действий этапа определения.

А.2.6 Заявление о соответствии

Независимо от того, участвуют ли в оценке соответствия другие стороны, всегда будет присутствовать некая форма заявления о соответствии поставщика продукта или услуги. Заявление может принимать форму рекламы или брошюры с описанием особенностей продукта или может быть включено в официальный документ, идентифицирующий поставщика и продукт, устанавливающий спецификации стандартов или других документов, соответствие с которыми было заявлено, возможно, особые правила, которым соответствует продукт и подпись ответственного лица. Даже размещение на продукте или приложении к нему имени поставщика, товарного знака или логотипа означает, что он соответствует спецификации поставщика. ИСО/МЭК 17050 (все части) предоставляет руководство по содержанию заявления о соответствии поставщика.

А.2.7 Определение. Условия проведения и методы тестирования

Руководство ИСО/МЭК 67 описывает семь основных типов систем сертификации продукции, отмечая, что элементы этих систем могут быть объединены другими способами для создания дополнительных систем. Эти системы могут включать в себя один или несколько следующих компонентов:

- образцы, запрашиваемые органом сертификации;
- определение соответствующих характеристик продукта путем проведения испытания (ИСО/МЭК 17025) или оценки;
- проведение аудита процесса производства или системы контроля качества;
- изучение отчетов оценки или испытания;
- подтверждение соответствия;
- выдача лицензии на использование сертификатов и знаков на продукции;
- контроль с помощью испытаний или проверки образцов с завода или рынка.

Опыт использования программ оценки соответствия четырех стран (в соответствии с описанием в настоящем приложении) показывает, что каждая применяла сочетание нескольких методов. Учитывая риски нарушения безопасности пациентов, страны все чаще переходят к сертификации продукции, проводимой уполномоченными третьими лицами, сосредотачиваясь на проведении оценки соответствия организациями, оказывающими медицинскую помощь, в которых должно использоваться и поддерживаться несколько программных продуктов, облегчающих обмен информацией о пациенте между пунктами оказания помощи для повышения безопасности пациента, качества и результатов. Так как используются все более сложные и межоперационные клинические системы POS, все больше и больше внимания также уделяется непрерывному наблюдению и повторной оценке систем, так как в экосистеме EHR происходят изменения программного обеспечения и стандартов. Во многих странах параллельное акцентирование внимания на управлении рисками нарушения безопасности пациента, связанными с медицинским программным обеспечением, также поможет снизить риски, связанные с контролем качества программного обеспечения, настройкой, реализацией и конечным пользователем.

А.2.8 Рассмотрение и аттестация

При функциональном подходе (см. рисунок 2) рассмотрение и аттестация представлены как совмещенная деятельность. Хотя возможно отдельное выполнение каждого из них разными лицами. Важно то, что ни одно действие не должно быть осуществлено лицом, которое участвовало в действиях этапа определения. Поскольку возрастает риск появления несоответствий, степень независимости рецензента увеличивается.

Рецензент должен обладать необходимой компетенцией по отношению к указанным требованиям, объекту оценки и действиям этапа определения, которые были использованы. Например, знание методик проведения испытаний позволит рецензенту определить несоответствующие результаты и передать отчет обратно лицу, проводившему испытание для повторного его проведения.

Заключением этапа рассмотрения является рекомендация о выдаче заявления о соответствии. Рекомендация должна содержать ссылку на отчет и любые другие выводы из обзора, которые подтверждают соответствие (или несоответствие) объекта указанными требованиями.

А.2.9 Управление версиями и надзор

В расширяющемся межоперационном мире EHR, где клинические системы POS имеют растущее количество точек взаимодействия (интерфейсов), с точки зрения информации (например, новые наборы кодов), политики (например, новые правила неприкосновенности частной жизни) и технологий важно иметь четкие правила, которые определяют необходимость переаттестации, когда происходят изменения в клинической системе POS или инфоструктуре EHR. Повторное испытание совместимости требует дисциплинированного проведения этого испытания с указанием того, какие изменения являются основными, а какие — второстепенными, а также с использованием средств для проведения испытаний и других механизмов, требующихся для того, чтобы сделать повторное испытание практичным и доступным во время сертификации.

Оценка соответствия может заканчиваться после выполнения аттестации, но в случаях, при которых существует необходимость непрерывного подтверждения соответствия, может использоваться надзор. Надзор систематически возобновляет деятельность по оценке соответствия, являясь основой для поддержания действительности заключения о соответствии. Как правило, нет необходимости в полном повторении первоначальной оценки при каждом цикле надзора для устранения данной необходимости.

В случае если объект признан несоответствующим, то лицо или организация, ответственная за объект, например инженер-разработчик, или в случае участия второй или третьей стороны — поставщик должны быть уведомлены и приглашены для внесения необходимых изменений для достижения соответствия. Важно, чтобы рецензент не предлагал возможные решения для того, чтобы не потерять свою объективность при возвращении объекта для дальнейшей проверки. Обсуждение результатов оценки признано допустимым для того, чтобы ответственное лицо или организация смогли понять причину несоответствия.

Обеспечение постоянного соответствия в более сложной и межоперационной экосистеме EHR является постоянной проблемой для поставщиков систем, покупателей и органов по сертификации, каждый из которых несет ответственность за проведение соответствующих мероприятий по оценке соответствия в своих средах. В дополнение к совместным и практичным процессам для снижения и управления рисками совместно с поставщиками и разработчиками программного обеспечения, возникновение которых связано с внесением изменений

в продукт, необходимы рациональные правила, которые позволят органам по сертификации, основываясь на принципах, определять степень повторного тестирования, необходимого при внесении изменений. Наконец, надежная система наблюдения, которая включает в себя внимательность поставщиков, разработчиков и конечных пользователей этих систем, а также эффективную систему предоставления отчетности, является важным компонентом.

А.2.10 Обучение, продажа и осуществление связи

А.2.10.1 Декларация о соответствии

Заключение о соответствии, выданное первой стороной, например поставщиком продукта, или второй стороной, например покупателем, называется декларацией о соответствии.

А.2.10.2 Сертификат соответствия

Заключение о соответствии, выданное третьей стороной (органом сертификации), является сертификатом соответствия. Однако используемые термины и конкретное содержание могут меняться в зависимости от оцениваемого объекта и характера указанных требований.

А.2.10.3 Знак соответствия

Как правило, продукты имеют знаки соответствия независимо от того, является этот знак собственным товарным знаком поставщика, сертификационным знаком, контролируемым органом по сертификации, или знаком соответствия, требуемым законодательством, например, маркировка CE Евросоюза. Рекомендации о знаках соответствия содержатся в ИСО/МЭК 17030 и Руководстве ИСО 27. Знаки должны иметь отличия, а их собственник и условия использования должны быть четко определены.

В частности, использование знака не должно вводить в заблуждение покупателей и пользователей продукта. Например, поставщик, который имеет сертифицированную систему менеджмента, соответствующую требованиям стандарта ИСО 9001, не должен ставить на свою продукцию знак органа по сертификации, так как это означало бы, что продукция сертифицирована органом.

Часто использование знака соответствия контролируется с помощью лицензии, выдаваемой владельцем знака или организацией, действующей от имени владельца, например, органом по сертификации. В лицензии излагаются условия, при которых лицензиат может использовать знак, например, ограничения, касающегося использования его только на тех продуктах, которые поставщик проверил на соответствие сертифицированному типу продукта. Определение политики использования знаков соответствия является жизненно важным для владельца и лицензирующего органа, так как продукция с их знаком часто производится в соответствии с системой, в которой лицензирующий орган проводит проверку только случайных образцов продукта.

С учетом этих принципов были разработаны четыре национальные программы по сертификации медицинского программного обеспечения.

А.3 Пример 1. Великобритания

А.3.1 Обзор и цели программы сертификации

Описание в этом разделе относится к режиму управления информацией, существовавшему в Национальной службе здравоохранения Великобритании в 2010 г. В то время, когда была написана эта техническая спецификация, режим управления информацией для Национальной службы здравоохранения Великобритании пересматривался. Результаты этого процесса дадут возможность для дальнейшего согласования, когда настоящий стандарт будет впоследствии подвергнут пересмотру со стороны ИСО.

Объединение здравоохранения [Connecting for Health (CFH)] Национальной службы здравоохранения Великобритании, являясь частью Департамента управления информатизацией здоровья (Department of Health Informatics Directorate), осуществляет централизованные процессы обеспечения безопасности, направленные на обеспечение:

- соответствия требованиям государственных контрактов ИТ службы NHS, т. е. контрактов местных поставщиков услуг (LSP), например CSC, контрактов государственных поставщиков услуг (NASP), например BT Spine, структуры GP Systems of Choice (GPSoC) и Каталога дополнительных услуг (ASCC);
- соответствия требованиям, принадлежащим CFH NHS, по требованию служб всех уровней, например службы хранения персональных демографических данных (PDS), управления информацией (IG), а также соответствия более сложным клиническим требованиям, таким как краткая история болезни (SCR) и служба электронных медицинских рецептов (EPS);
- соответствия любых систем, требующих подключения непосредственно к национальной программе Spine, как минимум требованиям управления информацией (IG) и как минимум еще одному набору требований, чтобы иметь некоторые функциональные возможности, требующиеся этим системам для того, чтобы быть подвергнутым этим процессам.

Общим процессом обеспечения безопасности (Common Assurance Process, CAP) является процесс обеспечения соответствия требованиям для CFH NHS в согласии с требованиями ко всем контрактным решениям, не относящимся к LSP и NASP. Решения LSP и NASP имеют свои конкретные контрактные процессы обеспечения безопасности, основанные на тех же принципах, что и CAP. Общий процесс обеспечения безопасности регулируется на операционном уровне Комитетом по операциям CAP. Данный комитет состоит из менеджеров всех сторон, участвующих в обеспечении безопасности. Этот Совет отправляет отчеты в Программный совет, который созывается

в исключительных ситуациях. Затраты, необходимые для реализации CAP в конкретном случае, должны быть включены в отдельные бизнес-модель программы/проекта и программу ее реализации.

А.3.2 Область применения рассматриваемых систем

Любая система, независимо от медицинского учреждения, которая требует подключения к национальной (EHR) системе, должна поддерживать процессы обеспечения качества. Существует более 80 систем, использующих процессы обеспечения безопасности во многих учреждениях, включая места оказания первичной медицинской помощи, неотложной медицинской помощи, социальной помощи, детские медицинские учреждения, места проведения клинических лабораторных исследований, рентгенограммы.

А.3.3 Ряд включенных клинических, административных, нефункциональных требований и требований к совместимости

Этот ряд зависит от того, что необходимо для решения, учитывая, что для конкретных услуг определены конкретные требования. Тем не менее процесс обеспечения клинической безопасности является общим для всех, и каждая система должна отвечать требованиям управления информацией для обеспечения безопасности и конфиденциальности.

Соответствие следующим основополагающим модулям является необходимым условием для применения в процессе сертификации для любых национальных служб EHR (бизнес-сфер), таких как выбор и регистрация, соответствие реферера или электронные рецепты. Основополагающими модулями в порядке очередности являются:

- управления информацией (IG);
- инфраструктура системы медицинских карт (CRS) (например, центр National Spine) и стандарты;
- служба хранения персональных демографических данных (PDS).

Данные модули содержат набор общих требований, применимых ко всем системам и стремящихся к соответствию с бизнес-сферой. Все эти основополагающие модули являются обязательными.

Соответствие может требоваться для бизнес-сфер и основополагающих модулей вместе или может достигаться отдельно.

Требования принципов управления информацией (безопасность и конфиденциальность) охватывают:

- аутентификацию программы Spine — поддержку однократной идентификации и смарт-карт, интеграцию с Spine Security Broker (посредником безопасности Spine) (SSB) CRS NHS и управление сеансом spine;
- локальную аутентификацию при отсутствии смарт-карт или SSB;
- ролевое управление доступом (RBAC) — поддержку национального сборника ролей и действий для осуществления санкционированного доступа к функциям системы и данным, где данные RBAC поступают от операторов SAML (язык разметки, предусматривающий защиту данных) и/или SDS и локальных требований RBAC при отсутствии смарт-карт или SSB;
- согласие — для разрешения разглашения персональной конфиденциальной информации о пациенте, находящейся в CRS NHS;
- службу родства, установленного законом (LRS) — для осуществления пользователем санкционированного доступа к персональным медицинским картам;
- метод запечатанных конвертов — позволяет пациентам осуществлять выбор уровня «видимости» хранимой информации о них;
- подтверждение содержания — допускает использование электронного аналога собственноручной подписи;
- ведение журнала аудита — записывает действия пользователя относительно личных данных CRS NHS;
- IT-безопасность — присвоение временных меток, хранение, тестирование, средства связи и средства управления доступом;
- систему менеджмента информационной безопасности — предоставляет соответствующие структуры и процессы управления.

А.3.4 Установление и поддержание требований, на соответствие которым проводится сертификация

Требования безопасности и конфиденциальности принадлежат команде IG SME технического отдела и обновляются каждый год, так как обновляется справочная документация, включаются разъяснения, запрашиваемые поставщиками, и должны учитываться технические изменения. Предлагаемые изменения в основном обуславливаются опытом использования процесса обеспечения безопасности по требованиям, хотя некоторые из этих изменений возникали в результате изменения политики вариантов согласия, предлагаемых пациентам, и т. д. Несколько лет назад отправной точкой для этого послужил набор требований по управлению безопасностью и информацией, изложенный в начале Национальной программы по ИТ.

А.3.5 Продолжительность сертификации и управление новыми версиями

Термин «сертификация» применяется к конкретной версии, он не зависит от времени. Ни одна система не остается неизменной в течение долгого времени, изменения либо вносятся поставщиками, например для выпуска версий с исправлением ошибок, либо служат для внесения дополнительных функциональных возможностей, связанных с программой Spine. В связи с этим CAP принимает решения о том, до какой степени статус обеспечения безопасности продукта должен быть повторно проверен. В будущем, когда значительные изменения, связанные с CFH, смогут уменьшаться в числе и частоте поступления, будет целесообразно рассмотреть повторную проверку, проводимую по времени.

А.3.6 Процесс проверки на соответствие

Процесс проверки начинается с продавца на стадии проектирования. Испытание проводится в тестовых средах NICA, что приводит в контролируемых условиях производства к «первой данного типа» реализации. Временные рамки зависят от поставщика в приведении его системы в то состояние, в котором она допускается в среду комплексных испытаний, и того какое время может занять испытание.

Существует исходная опубликованная версия «Принципов управления безопасностью и информацией», которая отражает особые требования программы, такие как аутентификация смарт-карт, а также руководство, соответствующее промышленным стандартам, например, по криптографическим алгоритмам для защиты данных при передаче и при бездействии. Мы включаем испытание на возможность проникновения в систему прикладного уровня для того, чтобы охватить более общие потенциальные проблемы, связанные с программным обеспечением. Все это находится на системном, программном уровне. На организационном уровне как для организаций-поставщиков, так и для организаций-пользователей существует отдельный процесс — формирование заявления о соответствии принципам управления информацией, включающий набор средств управления информацией для получения соответствия с ИСО/МЭК 27001.

А.3.7 Краткое описание текущих знаний

NHS использовала программу CAP в ее существующей форме в течение примерно пяти лет, в течение этих лет процессы были настроены и обновлены, но существенно не изменились. Опыт Великобритании заключается в том, что важно развивать тесные рабочие отношения с каждым поставщиком систем, начиная обсуждения на стадии проектирования, на которой предусматриваются изменения в клинической системе POS или национальной инфоструктуре EHR. Сотрудники CAP предоставят поставщику рекомендации, но так, чтобы не стать проектировщиками. После того как система была сертифицирована, результаты деятельности поставщика вместе с ожидаемым масштабом изменений учитываются при определении уровня повторного тестирования, которое должно быть выполнено CAP для поддержания сертификации клинических систем POS. В настоящее время необходимо рассмотреть способы, при которых процесс может быть четко организован в некоторых из ситуаций, например, путем предоставления возможности проведения большего количества процессов CAP на основе самостоятельного аудита тем поставщикам, которые имеют большой опыт и надежные процессы для достижения соответствия требованиям CAP.

Делая упор на локальную интеграцию «система — система» на уровне организации, предоставляющей медицинские услуги, разрабатывается дополнительный подход — процесс аккредитации набора средств для обеспечения интероперабельности (ITK). Однако ITK фокусируется только на функциональности интерфейса для обмена информацией и не включает в себя управление этой информацией (аутентификацию, аудит, согласие), клиническую безопасность, нефункциональное испытания, возможность подключения и взаимодействия (связность) для национальной EHR (Spine) или общую функциональность приложения. При таком подходе поставщикам систем предоставляются тестовые программы и тестовые сценарии для того, чтобы продемонстрировать свое соответствие требованиям «первой стороны».

А.4 Пример 2. Бразилия

А.4.1 Обзор и цели программы сертификации

В Бразилии существует единая национальная программа сертификации систем электронных медицинских карт (EHRs), стандарты и требования которой были определены Бразильским обществом по медицинской информатике (Sociedade Brasileira de Informatica em Saúde — SBIS) под руководством Федерального совета медицины Бразилии (Conselho Federal de Medicina — CFM), федерального агентства, ответственного за управление и надзор за медицинской практикой в стране. В Бразилии нет программ регионального или местного уровня. Эта программа была запущена в 2002 г. путем создания рабочей группы для согласования необходимых процессов и требований. Изначально группа опубликовала документ под названием «Требования к безопасности, содержанию и характеристикам систем электронных медицинских карт» (Safety, Content and Features Requirements for Electronic Health Record Systems), который после изменения в 2008 г. стал называться «Руководством по сертификации для систем электронных медицинских карт» (Certification Manual for Electronic Health Record Systems). Издание 2009 г. действует на данный момент, а издание 2010 г. находится на стадии разработки.

Бразильская программа контролируется и используется Бразильским обществом по медицинской информатике (Brasileira de Informatica em Saúde — SBIS), являющимся некоммерческим научным обществом, находящимся под руководством Федерального совета медицины Бразилии (Conselho Federal de Medicina — CFM), федерального агентства, ответственного за управление и надзор за медицинской практикой в стране.

А.4.2 Область применения рассматриваемых систем

Программа сертификации Бразилии в настоящее время ориентирована на системы для амбулаторного/поликлинического обслуживания. Позднее будут добавлены категории для больничного/стационарного лечения и для управления электронным информационным наполнением (electronic content management, ECM). В ближайшие годы будут добавлены другие новые категории.

А.4.3 Набор включенных клинических, административных, нефункциональных требований и требований к совместимости

Категория амбулаторного лечения имеет 113 установленных требований, разделенных на следующие группы.

Требования к структуре и содержанию:

- структура EHR;

- структурированные данные;
- административные данные;
- клинические данные;
- типы данных;
- справочные данные;
- контекстуальные данные;
- связки;
- представление медицинских понятий;
- представление текста.

Требования к характеристикам:

- поддержка клинических процессов;
- медицинские проблемы и другие вопросы;
- клиническое обоснование;
- поддержка принятия решений, клинические протоколы и предупреждения о возможной ошибке;
- планирование лечения;
- команды и сервисные процессы;
- комплексное лечение;
- обеспечение качества;
- сбор данных;
- извлечение, запросы и отображение данных;
- представление данных;
- масштабируемость и производительность;
- протоколы сообщений;
- обмен записями;
- согласие;
- судебно-медицинские требования;
- инстанции;
- клиническая компетенция и принципы управления;
- точность;
- сохранение контекста;
- стабильность;
- управление версиями;
- этика;
- права пациента;
- вопросы культуры;
- развитие.

Требования безопасности и конфиденциальности были разработаны на двух уровнях:

a) уровень обеспечения безопасности 1 (на португальском: Nvel de Garantia de Segurança 1 — NGS1);

b) уровень обеспечения безопасности 2 (на португальском: Nvel de Garantia de Segurança 2 — NGS2).

NGS1 применяется к местным или сетевым системам, которые не обеспечивают использование цифровых сертификатов и вследствие этого не допускают отказа от карт на бумажном носителе. Каждая сертифицированная система должна соответствовать как минимум на данном уровне. Он состоит из 53 требований, разделенных на следующие группы:

- управление версиями программного обеспечения;
- идентификация и аутентификация пользователя;
- управление сеансами пользователя;
- разрешение и контроль доступа;
- доступность EHR;
- удаленная связь;
- защита данных;
- аудит;
- документация;
- время;
- уведомление о событиях.

NGS2 применяется к системам, обеспечивающим использование цифровых сертификатов для аутентификации и подписания, и, следовательно, допускает отказ от карт на бумажном носителе. Данный уровень является необязательным и в надлежащем случае должен применяться в дополнение к NGS1. Он состоит из 25 требований, разделенных на следующие группы:

- цифровой сертификат;
- цифровая подпись;
- аутентификация пользователя с использованием цифрового сертификата;
- сканирование документа (для дальнейшего использования с категориями ECM).

А.4.4 Создание и поддержание требований, на соответствие которым проводится сертификация

Большинство требований безопасности и конфиденциальность основывались на стандартах ИСО, в частности ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 15408 (все части).

Федеральный совет медицины Бразилии предоставил начальные средства в размере 100 000 долларов США для разработки программы, притом что основная часть работы проводилась на добровольной основе группой акционеров SBIS. В настоящее время часть работы все еще выполняется добровольцами, а другая часть финансируется за счет оплаты обучающих курсов, предоставляемых SBIS, и сборов, оплачиваемых поставщиками за проведение аудитов. Набор требований по сертификации был создан и поддерживается рабочей группой, образованной членами SBIS, и основан на национальных и международных стандартах, в дополнение к правилам к национальным программам и соответствующему законодательству. Перед публикацией набор требований подвергался публичному рассмотрению, во время которого любое заинтересованное лицо или специалист может оставить комментарий или предложить внести изменения в предлагаемые тексты. После согласования и доработки SBIS публикует требования в качестве нового издания «Руководства по сертификации».

А.4.5 Продолжительность сертификации и управление новыми версиями

Утвержденные системы получают сертификат и печать, которые могут быть использованы продавцом в рекламных материалах в соответствии с критериями «Руководства по сертификации» и договором между поставщиком и SBIS.

Каждый сертификат действителен в течение двух лет, за исключением тех случаев, когда он отменяется в связи с любым нарушением правил программы. В течение этого периода повторные испытания не проводятся, так как сертификат присваивается конкретной системе определенной версии и в соответствии с определенным изданием требований. Поставщик обязан предоставить такую информацию в своих рекламных материалах и при реализации продукции на рынке или должен четко указать имя и версию сертифицированной системы, а также год издания требований, в котором была проведена проверка соответствия.

В случае если поставщик хочет продлить действие сертификата для новой версии системы, будут проводиться новые испытания, и после подтверждения соответствия сертификат будет продлен для новой версии. Однако это действие не является обязательным, и поставщик может поддерживать старую сертифицированную версию без сертификации новой.

После истечения срока действия поставщик может подвергнуть систему новому процессу аудита с последующим получением в случае удачной проверки нового сертификата на нее.

А.4.6 Процесс проверки на соответствие

Испытания, используемые во время сеанса аудита, выполняются при личной встрече в офисе SBIS в г. Сан-Паулу при участии трех аудиторов и трех специалистов поставщика, а средняя продолжительность испытания составляет три дня для каждой оцениваемой системы. Сеансы записываются, включая запись видеоматериала, отображаемого проверяемой системой, и запись звука в помещении на DVD-диски, которые хранятся в SBIS, для использования при согласовании консультации в случае, если результаты спорны.

Аудит использует тестовые сценарии, определенные в «Руководстве по проведению испытаний и анализов для сертификации EHRS», составленном SBIS вместе с «Руководством по сертификации». После запуска сценариев аудиторы проводят проверку соответствия системы каждому обязательному требованию из перечисленных категорий, предоставляя конечный результат после завершения испытаний.

Для того чтобы получить сертификат, система должна продемонстрировать соответствие всем обязательным требованиям перечисленных категорий; в ином случае сертификат не будет выдан. В случае несоответствия разработчик может применить дополнительный сеанс аудита (второй цикл) в течение 90 дней, считающийся «вторым шансом», для устранения обнаруженных неисправностей и повторного предоставления системы с необходимыми поправками.

После окончания сеанса аудита результаты, полученные аудиторами (первый уровень), предоставляются менеджеру процесса сертификации (второй уровень), который оценивает их и передает комитету по сертификации (третий уровень), включающий трех человек, которые следят за тем, чтобы весь процесс проводился в соответствии с правилами программы. После одобрения Комитет по сертификации выдает свидетельство и печать для системы, прошедшей оценку. В ином случае разработчик получает уведомление об отказе с указанием соответствующих причин.

Учитывая, что все этапы должны быть выполнены с момента вступления системы в программу до оглашения окончательного решения комиссии, каждый процесс занимает около 60 дней при условии, что второй цикл аудита (описанный выше) не требуется.

А.4.7 Краткое описание текущих знаний

Теория и практика, как правило, отличаются, это, конечно, касается и оценки соответствия систем EHR. Некоторые из первоначально разработанных требований, правил и процессов должны быть пересмотрены в процессе реализации, иногда в отношении концепции, в других случаях — в режиме выполнения и в отношении документации. Программа сформировалась и продолжает развиваться.

Несколько основных вопросов были изучены в Бразилии до настоящего времени:

- Существует возможность создания и внедрения национальной программы сертификации высокого качества, даже при ограниченных ресурсах и в большой стране. Мы обнаружили несколько препятствий при данном способе, но не было ни одного такого, которое мы не смогли преодолеть.

- Внедрение национальных и международных установленных стандартов имело решающее значение для успеха нашего проекта.

- Операционные процессы стандарта должны быть адаптированы под национальные и медицинские характеристики, особенно под их культурные и экономические условия. Успешные случаи в других странах или секторах не обязательно будут применимы в нашем проекте. Таким образом, мы адаптировали работу программы к нашим условиям, которые имели решающее значение для достижения положительных результатов.

- Радикальные и внезапные изменения в секторе здравоохранения могут разрушить весь проект. Поэтапное внесение изменений очень эффективно и содействует успеху программы.

Конечно, большое влияние, оказанное программой сертификации Бразилии по настоящее время, было подтверждением того, что содействие качественным скачкам на рынке систем электронных медицинских карт в стране представляется действительно возможным. По причине того, что программа сертификации фактически никогда не проходила апробацию с начала ее существования, большинство разработчиков до недавнего времени утверждали, что ее использование не приведет ни к каким результатам, что это будет нереальный и неосуществимый процесс и что ни один поставщик или компания-потребитель не обратят на нее внимания. Сейчас, спустя почти восемь лет с момента начала деятельности и почти два года с момента ее эффективной реализации, мы можем заявить, что программа сертификации имеет несомненный успех, учитывая высокий уровень мобилизации индустрии медицинских систем и приверженность процессу адаптации наших систем к требованиям, выставленным к программе. Фундаментальные принципы безопасности, конфиденциальности и содержания, ранее не учитывавшиеся в большинстве систем, стали согласовываться и реализовываться в большем масштабе, заставляя нас верить в возможность достижения действительно высокого уровня систем EHR в стране через несколько лет.

В результате данного качественного скачка, учреждения и медицинские работники начали получать выгоду от использования более совершенных и безопасных систем. Со временем станет проще и безопаснее выбрать решение EHR по снижению рисков перед тем, как с ними столкнутся пользователи этих систем. В конечном итоге мы будем совершенствовать процессы здравоохранения, поддерживаемые этими решениями. Все это уже начато и будет продолжаться еще более интенсивно, так как процесс эволюции не обратим.'

А.5 Пример 3. Канада

А.5.1 Обзор и цели программы сертификации

В Канаде федеральное правительство разрабатывает общенациональную политику в области здравоохранения, включая определение единого комплекса медицинских услуг, общедоступных во всей стране. Федеральное правительство работает в тесном сотрудничестве с провинциями и территориями, каждая из которых отвечает за предоставление медицинских услуг в пределах своей юрисдикции. В 2000 г. федеральное правительство в сотрудничестве с провинциями и территориями Канады разработало независимое агентство — канадскую медицинскую организацию Infoway, предназначенную для согласования последовательного подхода к реализации систем электронных медицинских карт в Канаде. Infoway разработала общую структуру EHR, являющуюся основным аспектом в разработке пан-канадских стандартов, и обеспечивает финансирование для поддержки провинций и территорий в реализации систем электронного учета здоровья (EHR), которые следуют данной структуре и необходимым стандартам совместимости. Одной из услуг, предоставляемой организацией Infoway, позволяющей поставщикам программного обеспечения, предоставляющим компоненты электронного учета здоровья (EHR), подтверждать их соответствие национальным медицинским ИТ-стандартам, является сертификация.

Целями службы сертификации Infoway являются:

- повышение уровня признания, принятия и внедрения надежных, совместимых решений по медицинской информации на канадском рынке;
- снижение стоимости и рисков для поставщиков, покупателей и пользователей данных решений в Канаде;
- обеспечение соответствия требованиям неприкосновенности частной жизни, безопасности и совместимости.

А.5.2 Область применения рассматриваемых систем

Программа сертификации, разработанная в 2009 г. канадской медицинской организацией Infoway, первоначально была сосредоточена на предварительной реализации нового перспективного поколения систем — пользовательских медицинских платформ. На сегодняшний день был сертифицирован один продукт — канадская реализация платформы Microsoft HealthVault.

За последние два года были разработаны программы сертификации для компонентов EHR в соответствии со структурой и схематическим планом Infoway. К таким компонентам относятся:

- пользовательское медицинское приложение (Nov 2009);
- реестр клиентов (Nov 2009);
- реестр провайдеров (Nov 2009);
- реестр вакцинации (Nov 2009);
- система информации о лекарственных средствах (July 2010);
- диагностическая визуализация/система передачи и архивации изображений (PACS)/радиологическая информационная система (RIS) (July 2010);
- другие компоненты EHR, такие как архивы лабораторных данных, ожидаются.

Программа сертификации в настоящее время разрабатывается для первой основной группы (клинических) систем пунктов оказания помощи — электронных медицинских карт (EHR) для того, чтобы во время предварительной реализации предоставить гарантию их совместимости с точки зрения конфиденциальности и безопасности с инфраструктурой EHR Канады, иметь возможность предоставления доступа к лабораторным и диагностическим результатам пациента, выписывать электронные рецепты и предоставлять доступ к карте назначений пациента, записывать прививки, а также обеспечивать доступ к текущему прививочному статусу пациента, и т. д.

Кроме того, ожидается, что программа сертификации Infoway начнет включать некоторые компоненты совместимости систем EHR-EHR (например, обмен электронными направлениями к врачу eReferrals между врачами общей практики и специалистами в 2012 г.).

Несколько провинций также разработали непрерывные процессы проверки соответствия и требования к EHR, которые будут подключаться к каждому экземпляру инфраструктуры EHR провинции (или территории). Эти процессы оценки соответствия рассматривают взаимодействие на более детальном уровне с точки зрения использования и поддержания постоянной интеграции EHR и инфоструктуры EHR в пределах системы здравоохранения каждой области. В настоящее время между организацией Infoway и областями, которые реализовали процессы оценки соответствия на уровне своих юрисдикций, ведутся обсуждения с целью унифицировать требования, процессы и наборы тестовых данных и достигнуть максимально возможного взаимопонимания для того, чтобы поставщикам программного обеспечения не пришлось проводить повторную проверку своих систем без необходимости.

А.5.3 Набор включенных клинических, административных, нефункциональных требований и требований к совместимости

Критерии оценки сертификации Infoway сосредоточены на функциональности, конфиденциальности, безопасности, совместимости и управлении, используя утвержденные стандарты канадских и международных комитетов по медицинской информации, а также усилены данными и комментариями множества заинтересованных лиц индустрии здравоохранения.

Основа для критериев оценки приведена в таблице А.1. Она состоит из двух классов критериев:

- Решение. Относится к оцениваемым аспектам функциональности решений по медицинской информации, конфиденциальности, безопасности и совместимости;
- Управление. Касается того, как организация, предоставляющая решение, управляет рисками, данными и безопасностью системы, а также услуг третьих лиц и аккредитации решения.

Таблица А.1 — Основа для критериев оценки

Решение «Что»				Управление «Как»
Функциональность	Конфиденциальность	Безопасность	Совместимость	Контроль
Идентификация	Отчетность	Управление идентификационной информацией пользователя	Диагностическая визуализация	Управление рисками
Точность данных	Прозрачность	Контроль доступа	Лаборатория	Управление данными
—	Средства защиты данных	Целостность данных	Лекарственные препараты	Безопасность системы
—	Определение целей и ограничение сбора	Доступность данных	Общедоступная медицинская карта	Аккредитация решения
—	Ограничение использования, разглашения и сохранения	Аудит	Демографические данные клиента	Услуги третьих сторон
—	Соответствие	Ведение журнала	Демографические данные провайдера	—
—	Согласие	Конфиденциальность данных	—	—

Примечание — Добавление ограниченного количества дополнительных функциональных критериев может быть необходимо в зависимости от требований класса каждого технологического решения.

А.5.4 Основа стандартов сертификации

Стандарты, использованные для создания критериев оценки, включают:

- Функциональность. Требования к безопасности и конфиденциальности электронных медицинских карт канадской медицинской организации Infoway;

- Конфиденциальность. Концептуальная структура конфиденциальности и безопасности инфоструктуры электронного учета здоровья (Инфоструктура EHR) канадской медицинской организации Infoway; Закон правительства Канады о защите персональных данных и электронных документов (PIPEDA); Типовой кодекс канадской ассоциации по стандартизации о защите персональной информации — CAN-CSA-Q830-03;

- Безопасность. Концептуальная структура конфиденциальности и безопасности инфоструктуры электронного учета здоровья (Инфоструктура EHR) канадской медицинской организации Infoway; Свод норм и правил менеджмента информационной безопасности Международной организации по стандартизации — ИСО/МЭК 27002; Рекомендуемые средства управления безопасностью для Федеральных информационных систем Национального института стандартов и технологий — NIST SP800-53; Правило защищенности закона США о сохранении медицинского страхования и персонифицированном учете в здравоохранении (HIPAA);

- Совместимость. Пан-канадские стандарты Infoway и определения профилей соответствия для диагностической визуализации, лабораторных данных, информации о лекарственных препаратах, общедоступных медицинских карт и демографических данных;

- Управление. Задачи информационных и смежных технологий Института управления ИТ (COBIT); Библиотека инфраструктуры информационных технологий (ITIL).

А.5.5 Установление и поддержание требований, на соответствие которым проводится сертификация

Требования безопасности и конфиденциальности принадлежат и к группе по сертификации из канадской медицинской организации Infoway и поддерживаются ею. Требования поддерживаются и обновляются в соответствии с пан-канадскими стандартами, установленными группой Infoway Standards Collaborative, которая состоит из заинтересованных сторон провинциального и национального уровня из государственных органов, медицинских учреждений, профессиональных групп и поставщиков медицинских систем.

А.5.6 Процесс сертификации

Процесс сертификации состоит из четырех этапов:

a) Приложение по сертификации. В комплекте имеется:

- приложение для бланка сертификации;

- самооценка (которая должна быть завершена и представлена как часть прикладного процесса);

- копия сертификационного правового соглашения на предпроектной стадии.

b) Оценка продукта. Оценка продукта является важным этапом процесса сертификации, и поставщик должен в течение 90 дней с момента получения пакета прикладных программ завершить данный этап, который включает:

- Обзор документа. Административная и экспертная проверка самостоятельной оценки поставщика и подтверждающей документации;

- Демонстрация. Предоставление поставщиком решения экспертам, подтверждающее соответствие критериям оценки, как правило, посредством проведения веб-конференции и демонстрационной среды;

- Отчет по оценке. Infoway соберет результаты оценки во всесторонний отчет и уведомит поставщика в течение пяти рабочих дней со дня принятия решения по сертификации;

- Поддержка. Для поддержки сертификации поставщик обязан уведомить Infoway о неблагоприятных событиях, а также о любых изменениях продукта, которые могут повлиять на соответствие критериям оценки.

Процесс сертификации строго конфиденциален. Названия продуктов и/или поставщиков не публикуются или иным образом предоставляются организацией Infoway в любое время в ходе процесса. Средства защиты были введены в действие для того, чтобы использование и разглашение всей информации, представленной в процессе сертификации, включая название продукта, производителя, самостоятельную оценку и любую вспомогательную документацию, представленную в ходе процесса, оставалось строго конфиденциальным. Кроме того, оценочная группа по сертификации связана строгими соглашениями о неразглашении информации. Infoway публикует только названия тех продуктов, которые успешно прошли сертификацию, с указанием подробной информации о том продукте, который размещен на веб-сайте Infoway.

Все сертифицированные продукты получают сертификационный знак, на котором изображен логотип Infoway. Сертификационный знак может быть использован в маркетинговом и рекламном материале, связанном с сертифицированным продуктом.

А.5.7 Краткое описание текущих знаний

Infoway с момента своего основания не предусматривала финансирования для (клинических) систем POS, подключенных к провинциальным инфоструктурам EHR, несмотря на это, пан-канадские стандарты по совместимости, которые поддерживаются группой Standards Collaborative, возглавляемой Infoway, должны рассматривать клинические системы POS для совместимости с EHR. При канадском федеративном медицинском подходе, каждая провинция/территория реализовала данные стандарты, внеся локальные изменения, до принятия которых, как правило, в каждой провинции существовала устаревшая версия клинической системы POS.

В 2011 г., однако, Infoway начнет реализацию новой программы по обеспечению финансирования областей и регионов для того, чтобы дать толчок внедрению EHR в кабинеты врачей (которые будут использовать

пан-канадские стандарты для интеграции с областными инфраструктурами EHR); Infoway разработала спецификации и инструменты для того, чтобы оказать помощь поставщикам программного обеспечения клинической системы POS в реализации требований к конфиденциальности, безопасности и интерфейсу данных, используя пан-канадские стандарты и структуру конфиденциальности и безопасности Infoway. В этом случае функции конфиденциальности, безопасности и совместимости EHR будут сертифицированы организацией Infoway. В настоящее время между организацией Infoway и провинциями ведутся обсуждения для дальнейшего согласования способа, которым реализуются пан-канадские стандарты, а также большей унификации процесса сертификации предварительной реализации Infoway и проверки соответствия, которые инвестируются областями для обеспечения надлежащего взаимодействия (клинических) систем POS со своими инфоструктурами EHR.

Подводя итог, следует отметить, что в Канаде разрабатывается комбинация подходов по оценке соответствия, включая:

- сертификацию предпроектной стадии, разрабатываемую на национальном уровне канадской медицинской организацией Infoway для ряда EHR-сервисов, финансируемых Infoway, например, архивы данных и реестры, которые необходимы в провинциях, и

- программы оценки соответствия, разрабатываемые на областном/региональном уровне для обеспечения совместимости (клинических) систем POS, установленных во врачебных кабинетах, аптечных организациях и больницах, с каждой уникальной провинциальной версией EHR-инфраструктуры Infoway.

А.6 Пример 4. США

А.6.1 Обзор и цели программы сертификации

В Соединенных Штатах федеральное правительство играет важную роль в создании политики в области общественного здравоохранения и стандартов, а также в предоставлении медицинской помощи непосредственно определенным группам (например, для военнослужащих и ветеранов). Несмотря на то что медицинское обслуживание предоставляется большинству граждан через целый ряд общественных, некоммерческих и коммерческих организаций, федеральное правительство путем финансирования организаций здравоохранения через программы Medicare (федеральная программа медицинской помощи престарелым) и Medicaid (федеральная система медицинской помощи неимущим) получает значительное влияние благодаря установлению требований к денежным компенсациям и материальному стимулированию.

Учитывая важность повышения качества и стабильности здравоохранения и наличие многих препятствий при обмене медицинским данными между пунктами медицинского обслуживания, в которых пациенты проходят лечение, в связи с конкурентными, клиническими, административными и техническими препятствиями в феврале 2009 года Конгресс издал Закон о стимулировании медицинских информационных технологий для оздоровления экономики и медицины (HITEC) для того, чтобы повысить использование электронных медицинских карт (EHR) врачами и больницами, которым выделяется:

- 18 млрд долларов США через системы льгот Medicare и Medicaid для материального стимулирования больниц и врачей, являющихся «главными пользователями» систем EHR;

- 2 млрд долларов США Управлению национального координатора на инфраструктуру, необходимую для обеспечения и содействия электронному обмену и использованию медицинской информации каждого человека в Соединенных Штатах; на обновление технологий Министерства здравоохранения и социальных услуг для обеспечения электронного потока информации; на включение обучения медицинским информационным технологиям в программу подготовки работников здравоохранения, а также на содействие развитию совместимых архивов клинических данных;

- 1 млрд долларов США на обеспечение доступности медицинских центров для обновления и ремонта и на приобретение медицинских ИТ-систем;

- 550 млн долларов США (среди прочего) на закупку оборудования и услуг, включая, кроме прочего, медицинские информационные технологии в медицинских учреждениях Индии;

- 400 млн долларов США на исследование сравнительной эффективности того, как использование электронных данных влияет на методы лечения и стратегии в здравоохранении;

- 300 млн долларов США на поддержку региональных и суб-национальных усилий в области обмена информацией о здравоохранении;

- 40 млн долларов США для Администрации социального обеспечения, для использования EHR для подачи страхового требования по инвалидности;

- Управлению национального координатора по медицинским информационным технологиям (HIT) (ONC) было поручено утвердить первоначальный набор стандартов HIT и создать поощрительную программу для значащих пользователей сертифицированной технологий EHR. Управление национального координатора имеет два консультативных комитета, Комитет по политике HIT и Комитет по стандартам HIT;

- Комитет по политике HIT несет ответственность за предоставление национальному координатору по информационным технологиям в здравоохранении рекомендаций по основе политики разработки и принятию общенациональной медицинской информационной инфраструктуры, в том числе стандартов по обмену медицинской информацией;

- Комитет по стандартам HIT несет ответственность за предоставление национальному координатору по информационным технологиям в здравоохранении рекомендаций по стандартам, спецификациям реализации, а также критериям выдачи сертификата для электронного обмена и использования медицинской информации.

В июле 2010 г. Управление национального координатора выпустило окончательное правило, охватывающее исходные стандарты, спецификации реализации, а также критерии выдачи сертификата. Окончательное правило CMS содержит положения, регулирующие поощрительные программы EHR Medicare и Medicaid, и определяет разумное использование.

Учитывая спрос, предполагалось создание программ для сертифицированных систем: Организация ONC создала временную программу сертификации, по которой организации могут подать заявку на аккредитацию в качестве уполномоченного ONC органа сертификации и проведения испытаний (ONC-ATCB) для одного или более модулей (в том числе для таких областей, как выписка электронных рецептов, конфиденциальность и безопасность, лаборатории, качество и т. д.) в соответствии со стандартами и окончательным правилом по критериям сертификации. Кандидаты должны прилагать результаты самостоятельного аудита в соответствии с ИСО/МЭК 17065, помимо соответствия другими критериями. В настоящее время существует пять уполномоченных органов сертификации и проведения испытаний, одним из которых является Комиссия по сертификации в области медицинских информационных технологий (CCHIT), дополнительное описание которой приведено ниже. Нормативные критерии сертификации и методы проведения испытаний определены Национальным институтом стандартов и технологий (NIST).

Примечание — В январе 2011 г. Организация ONC выпустила окончательное правило для создания постоянной программы сертификации для информационных технологий в здравоохранении: «Постоянная программа сертификации предоставляет новые возможности, которые усовершенствуют сертификацию медицинских информационных технологий, а также повысят комплексность, незаметность, надежность и эффективность существующих процессов, используемых для сертификации технологий электронного учета здоровья (EHR). Разумное использование сертифицированных технологий EHR является основным требованием для соответствующих критериям лиц, предоставляющих медицинские услуги, которые стремятся к получению квалификации для получения поощрительных выплат по мотивационным программам электронного учета здоровья Medicare и Medicaid в соответствии с Законом о применении медицинских информационных технологий в экономической деятельности и клинической практике (HITECH). Нашей целью является осуществление как можно более плавного перехода на постоянную программу сертификации».

Национальный институт стандартов и технологий разработает программу аккредитации лабораторий для организаций, которые подлежат аккредитации, чтобы те могли получать разрешения на проведение испытаний медицинских информационных технологий для постоянной программы сертификации. «Основываясь на технической экспертизе NIST и крепких взаимоотношениях, образованных между ONC и NIST в процессе успешной реализации временной программы сертификации, можно полагать, что использование NVLAP (Национальной программы добровольной аккредитации лабораторий) повысит качество испытаний в рамках постоянной программы сертификации и их объективность в целом».

Особенностями постоянной программы сертификации являются:

- организации сначала должны быть аккредитованы с целью проведения испытаний и/или сертификации медицинских информационных технологий;
- органы сертификации должны осуществлять контроль после сертификации, выполнять «промежуточную сертификацию».

А.6.2 Область применения рассматриваемых систем

Сертифицированные EHR или модули являются сертифицированными и гарантируют, что они предоставляют необходимые технологические возможности, функциональность и безопасность для того, чтобы помочь лицам, предоставляющим медицинские услуги, достичь соответствия критериям «разумного использования» и получить стимулирующие выплаты. Включены как больничные, так и амбулаторные системы для клиник (ЭМЗ).

А.6.3 Набор включенных клинических, административных, нефункциональных требований и требований к совместимости

Требования охватывают ряд областей, включая:

- наборы основных данных для поддержки целого ряда клинических функций, таких как ведение перечня проблем и аллергических реакций, выписка рецептов, клинические меры качества/отчеты о качестве и обмен резюме клинических данных;
- демографические данные пациента и возможность предоставлять пациентам итоговую информацию об их визитах;
- защиту электронной информации о пациенте, которая включает более базовые элементы безопасности:
    - контроль доступа,
    - экстренный доступ,
    - автоматический выход из системы,
    - журналы аудита,
    - аутентификацию,

- кодирование.

В соответствии с ИТ-координатором в сфере общественного здравоохранения ожидается, что вторая стадия разработки требований к разумному использованию будет «рассматривать стандарты и критерии оценки, средства обеспечения защиты безопасности и конфиденциальности, методы управления обменом данных, доверительными фондами и интероперабельностью».

А.6.4 Продолжительность сертификации и управление новыми версиями

Поскольку сертификация в соответствии с окончательным правилом разумного использования предоставляется в рамках временной программы сертификации, существующие сертификаты не потеряют силу до момента реализации Постоянной программы сертификации, т. е. не раньше 1 января 2012 г.

Примечание — Комиссия CCHIT является одним из шести уполномоченных ONC органов сертификации (ATCB) в США и продолжает предоставлять услуги по своей традиционной сертификации CCHIT, основанной на более обширном наборе функциональных критериев. Сертификаты от 2011 г., предоставляемые комиссией CCHIT посредством внутренней программы, теряют силу 31 декабря 2014 г.

А.6.5 Процесс проверки соответствия

Органы ONC-ATCB должны использовать утвержденные ONC методы проведения испытаний, разработанные совместно с NIST, для проведения испытаний и сертификации технологий EHR в соответствии со стандартами, спецификациями по реализации и критериями сертификации, утвержденными руководителем. Национальный институт стандартов и технологии (NIST) совместно с ONC разработал требования к функциональным возможностям и проверке соответствия, тестовые сценарии и инструменты тестирования для поддержки предлагаемых программ сертификации медицинских информационных технологий. Данные методы проверки соответствия (процедуры испытаний, данные испытаний и инструменты тестирования) помогут обеспечить соответствие техническим требованиям и стандартам разумного использования.

А.6.6 Краткое описание текущих знаний

Правительство США за последние годы значительно усовершенствовало свой подход в результате создания Управления национального координатора (Office of the National Coordinator, ONC) и установления требований «разумного использования». Несмотря на то что программа сертификации США реализуется в несколько этапов и не полностью работоспособна, следующие элементы этого подхода являются наиболее уникальными:

- упор на разумное использование, которое акцентирует внимание на сборе, обмене и клиническом использовании информации для содействия усовершенствованию процесса слежения за болезнью, координирования медицинского обслуживания и поддержки принятия решений;
- подход, состоящий из трех этапов для прогрессирующей поддержки качества и безопасности медицинской системы и повышения эффективности, который включает в себя значительные финансовые поощрения для поставщиков и организаций, демонстрирующих внедрение и использование сертифицированных систем, а также адаптирует требования сертификации к конкретным типам медицинских систем;
- использование аккредитации в качестве механизма для создания многочисленных органов сертификации в сочетании с поэтапным подходом к реализации требований разумного использования предоставило возможность сертификации большого количества систем за относительно короткий период времени.

Приложение В
(справочное)

Сравнение требований юрисдикций

В.1 Общие сведения

В данном приложении сравниваются требования четырех отдельных национальных проектов по реализации EHR в Бразилии, Канаде, США и Великобритании. Кроме того, приведены отдельные требования Японии и Российской Федерации. Оно организовано по следующим категориям:

a) **Согласие пациента на сбор, использование или разглашение персональных медицинских данных.** включает регистрацию согласия, типы согласия, привязку согласия, игнорирование согласия в случае чрезвычайных обстоятельств, регистрацию случаев игнорирования согласия, маскировку данных, согласие, данное заменяющим ответственным лицом, а также оповещение пациентов об изменениях согласий.

b) **Ограничение использования и разглашения ПМД.**

c) **Доступ пациента к персональной информации и исправление неточных данных.**

d) **Точность данных.**

e) **Идентификация и аутентификация пользователей**, включая идентификацию пользователя, ID пользователей; аутентификацию пользователя; аутентификацию системой и аутентификацию сетевого узла; методы аутентификации; защиту профилей пользователя; пароли; неудачные попытки входа и обратную связь с пользователем во время аутентификации.

f) **Управление привилегиями,** включая разрешение на доступ, предоставление информации о правах доступа, ограничения прав на доступ, передачу прав на доступ и отмену права на доступ.

g) **Приемлемое использование**, включая уведомление пользователей.

h) **Безопасность сеанса и время ожидания**, включая пользовательские сеансы и время ожидания подключения, а также защиту сеанса.

i) **Поддержание доступности данных**, включая резервное копирование и восстановление.

j) **Защита данных в процессе передачи**, включая кодирование данных в процессе передачи и подтверждения доставки данных.

k) **Защита данных в процессе хранения**, включая защиту данных в архивах и защиту данных на портативных носителях.

l) **Целостность данных**, включая проверку целостности данных, целостность данных в ходе импорта данных и проверку исходящих данных.

m) **Хранение записей.**

n) **Маркировка данных.**

o) **Аудит**, включая журналы аудита и события срабатывания триггера, интерфейс, содержание, следственные инструменты, защиту, хранение, управление, постоянное ведение журнала аудита и восстановление содержания электронной медицинской карты на предшествующий момент времени.

p) **Управление версиями программного обеспечения и документация**, включая требования к управлению версиями ПО и документации.

q) **Синхронизация времени и форматирование времени/даты**, включая формат времени и синхронизацию времени.

r) **Контроль инцидентов нарушения безопасности и конфиденциальности.**

s) **Цифровые сертификаты и цифровые подписи**, включая использование цифровых сертификатов, цифровых подписей, предоставление цифровых подписей пользователям, формат подписи, проставление цифровой подписи, временные отметки, проверку достоверности цифровых подписей, роль подписывающего лица, экспорт документов и записей, содержащих электронную подпись, политику использования цифровых подписей и использование цифровой подписи на оцифрованных (отсканированных) документах.

В таблице, приведенной ниже, требования канадской медицинской организации Infoway относятся к централизованным юрисдикционным архивам медицинских записей (например, Центральному архиву электронных медицинских карт для жителей Манитобы). Требования Управления информацией Великобритании относятся к программе Spine и Службе данных пациента (Patient Data Service, PDS), они также относятся к централизованным юрисдикционным архивам записей (например, Центральный архив электронных медицинских карт для жителей Англии). Требования Бразилии относятся к процессам сертификации медицинского программного обеспечения, контролируемого бразильским обществом по медицинской информатике при поддержке палаты врачей.

В.2 Согласие пациента на сбор, использование или разглашение персональных медицинских данных

В.2.1 Регистрация согласий

Бразилия

NGS1.04.09 Ограничения доступа к EHR, добавленные пациентом:

Позволяет пациентам добавлять ограничения к части или всем EHR.

HL7 ERH-S FM IN1.4

Канада

Требование конфиденциальности 9 канадской медицинской организации Infoway

Регистрация согласия в системах POS

Системы POS, подключенные к инфоструктуре электронного учета здоровья в случаях, определенных законом, должны иметь возможность записи директив согласия пациента/лица, включая приостановку, отказ или аннулирование согласия.

Обоснование — Медицинские учреждения должны быть осведомлены о том, что они получили согласия, необходимые в их конкретных юрисдикциях для целей, в рамках которых они будут собирать, использовать или раскрывать ПМД (см. требование конфиденциальности 5, приведенное в разделе 5).

Форма согласия, запрашиваемая организацией, подключающейся к инфоструктуре EHR, может различаться, в зависимости от юрисдикции, обстоятельств, при которых была собрана информация (например, скорая медицинская помощь) и типа информации (например, обязательное уведомление об инфекционных заболеваниях). В канадской среде EHR необходимые формы согласия в основном утверждаются различными законами, в первую очередь законами о защите медицинских данных и о конфиденциальности государственного сектора. Те лица, которые вводят персональные медицинские данные в систему POS в конкретной юрисдикции, имеют основное обязательство по получению и записи директив согласия пациентов/лиц. Система POS должна гарантировать, что те, кто осуществляет доступ к этим ПМД, могут получить доступ только к той информации, которая доступна на законных основаниях, в соответствии с согласием или на основе законного разрешения на использование или разглашение (например, аудит или правоохранительные органы).

Требование конфиденциальности 11 канадской медицинской организации Infoway

Регистрация согласия в Инфоструктуре EHR

Инфоструктура EHR в случаях, определенных законом, должна иметь возможность регистрации директив согласия пациентов/лиц, включая приостановку, отказ или аннулирование согласия, а также должна выполнять это таким способом, который позволяет каждой юрисдикции соответствовать своим законодательным требованиям по согласию.

Обоснование — Медицинские учреждения должны быть способны определять, дал ли пациент/лицо разрешение или отозвал его, что соответствует требованиям в конкретных юрисдикциях этих учреждений.

Следовательно, те организации, которые собираются сообщить ПМД другой юрисдикции, должны делать это так, чтобы это не противоречило законодательным требованиям по согласию их собственной юрисдикции (т. е. юрисдикции разглашающей организации). На практике медицинская организация, желающая получить доступ к ПМД другой юрисдикции, должна делать это таким образом, который не противоречит законодательным требованиям по согласию на разглашение ПМД в юрисдикции организации, которая владеет данными, а также выполняет все законодательные требования по согласию на доступ к ПМД в их собственной юрисдикции. (В ином случае отправитель не может ответить на запрос доступа). Это приводит к глубоким последствиям, касающимся совместимости с инфоструктурой EHR. Информация, содержащаяся в EHR пациента/лица, может содержать правовые требования к согласию от нескольких юрисдикций (см. требование конфиденциальности 12, приведенное в разделе 5). Прежде чем разрешить доступ к ПМД инфоструктура EHR должна гарантировать, что все необходимые юридические требования выполнены перед передачей данных запрашивающему лицу.

Великобритания

Требование 3.2.2 Управления информацией (IG) Великобритании

Система должна предоставлять средство сбора информации о статусе согласия пациента и его решениях и, соответственно, обновлять PDS.

Требование 3.2.3 Управления информацией Великобритании

Система должна предоставлять пользователям возможность записи текстовых заметок на естественном языке о решении пациента или отсутствии его решения касательно обмена информацией по Spine, а также о процессе принятия решений. Во избежание неправильного толкования эта информация будет храниться локально, а не в Spine.

Требование 3.16.4 Управления информацией Великобритании

Доступ со стороны систем социальной помощи

Система должна обеспечивать возможность сбора текстовых заметок на естественном языке, связанных с процессом принятия решений. Система должна предоставлять возможность обеспечения дополнительной информации о механизме согласия и его влиянии на пользователя в рамках взаимодействия с клиентом.

Например, это может быть достигнуто с помощью системы, обеспечивающей функцию отображения пояснительного текста, который был создан организацией ранее.

Российская Федерация

Требование 13 закона РФ от 2011-11-21

Соблюдение врачебной тайны

Согласие пациента не требуется если:

- персональные медицинские данные обрабатываются для процессов контроля и управления государственного социального страхования;
- происходит обмен персональными медицинскими данными между медицинскими организациями для постановки диагноза или медицинского обслуживания;
- персональные медицинские данные используются для контроля качества и безопасности медицинского обслуживания.

В.2.2 Типы согласия

Великобритания

Требование 3.2.4 Управления информацией Великобритании

Собранная информация о состоянии согласия пациента должна включать указание о том, было ли принято «выраженное согласие», «несогласие» или «подразумеваемое согласие» пациента, и дату принятия данного решения.

Требование 3.16.2 Управления информацией Великобритании

Доступ из систем социальной помощи

Система должна предоставлять функциональные возможности для регистрации и записи статуса предпочтений лица, касающихся осуществления доступа к его картам, хранящимся в NHS, из учреждений социальной помощи, в которых в противном случае такой доступ может быть разрешен соответствующим зарегистрированным, аутентифицированным и авторизованным пользователям. Система должна проводить различие между типами согласия: «предпочтение не выражено», «выражено согласие» и «выражено несогласие». Стандартным значением для этого статуса, до того как была собрана любая информация об индивидуальном лице, должно являться «предпочтение не выражено». «Предпочтение не выражено» означает, что вопрос не был задан клиенту (и, следовательно, система может отправлять запрос в соответствующие точки). «Выражено согласие» позволяет системе осуществлять доступ к сервисам NHS (см. требование 3.16.7). «Выражено несогласие» означает события, при которых вопрос клиенту был задан, и клиент выразили свое предпочтение, и что, следовательно, новый запрос не может быть отправлен в ходе того же периода лечения (хотя новый запрос может быть уместен при проведении последующей значимой оценки). Клиент может обновить статус своего согласия в любой момент в ходе лечения.

Требование 3.16.3 Управления информацией Великобритании

Доступ из систем социальной помощи

Система должна поддерживать изменение статуса согласия лица с «предпочтение не выражено» на «выражено согласие» и «выражено несогласие». Если статусом является «выражено согласие», то он может быть изменен только на «выражено несогласие», а если статусом является «выражено несогласие» он может быть изменен только на «выражено согласие».

Требование 3.16.5 Управления информацией Великобритании

Доступ из систем социальной помощи

Система должна регистрировать личность пользователя системы, записывающей такие решения, с указанием времени, даты и местоположения. Система должна записывать идентификационные данные рабочей станции конечного пользователя или используемого устройства.

Требование 3.16.6 Управления информацией Великобритании

Доступ из систем социальной помощи

Система должна поддерживать и обеспечивать представление, историю решений, которые принимаются лицом, а также любых связанных с ними примечаний. Доступ к данной истории должен предоставляться только пользователям, обладающим особыми дополнительными правами.

Требование 3.16.7 Управления информацией Великобритании

Доступ из систем социальной помощи

Перед осуществлением любого доступа к PDS (или любым другим сервисам Spine, кроме поддержки аутентификации или RBAC) система должна установить, что текущим параметром предпочтения клиента является «выражено согласие». При отсутствии этого параметра ни один такой доступ не может быть осуществлен.

Требование 3.16.8 Управления информацией Великобритании

Доступ из систем социальной помощи

Явно выраженное согласие, описанное в данном пункте, должно подвергаться как минимум одной из трех следующих форм проверки:

а) Явно выраженное согласие в соответствии с описанием в данном пункте относится только к конкретному периоду медицинского обслуживания. Система должна гарантировать, что данное записанное согласие рассматривается только в контексте конкретного периода медицинского обслуживания (который, однако, может

быть многолетним). Это может поддерживаться путем связывания этого согласия с явным эпизодическим случаем, управляемым в пределах местной системы обслуживания, или (если согласие проводится по отношению к общей записи клиента) путем смены флажка согласия на «предпочтение не выражено» сразу после окончания периода медицинского обслуживания;

b) Любое явно выраженное согласие в соответствии с описанием в данном пункте может быть доступно для применения к клиенту в течение любых периодов медицинского обслуживания в будущем (за исключением случаев, когда оно аннулируется клиентом в любой момент) только в том случае, если выраженность была согласована с клиентом во время первоначального взаимодействия с ним для получения его согласия;

c) Записанный статус явно выраженного согласия в соответствии с описанием в данном пункте должен применяться только до выполнения любой последующей оценки со стороны социальной помощи (например, контактная или общая оценка SAP, при которой потребности здравоохранения и социального обеспечения оцениваются совместно), в результате которой указанный статус согласия должен быть подтвержден клиентом.

В отсутствие явного выражения клиентом согласия по этим принципам система должна поддерживать механизм обеспечения разрешения клиента, чтобы получить возможность доступа только на время сеанса регистрации для текущего пользователя.

В.2.3 Привязка согласия

Канада

Требование конфиденциальности 10 канадской медицинской организации Infoway

Связывание согласия с ПМД в системах POS

Если системы POS, связанные с инфоструктурой EHR, регистрируют директивы согласия пациента/лица, в том числе приостановку, прекращение согласия или отказ от согласия, такие системы POS должны передавать данные директивы согласия в инфоструктуру EHR в последовательной форме каждый раз при передаче связанных ПМД в инфоструктуру EHR.

Обоснование — Не во всех юрисдикциях требуется, чтобы система POS собирала директивы согласия. В случаях, при которых осуществляется сбор этих директив, важно, чтобы они передавались в инфоструктуру EHR каждый раз, когда должны передаваться связанные ПМД. Это обеспечит надлежащую обработку данных директив согласия инфоструктурой EHR перед передачей ПМД в другую юрисдикцию. Обратите внимание на то, что задача по обеспечению соответствия с требованиями других юрисдикций переходит от системы POS к инфоструктуре EHR, что является разумным подходом, учитывая большое количество юрисдикций и согласия разной сложности между ними.

Стандарты и форматы таких данных согласия, не входят в объем и содержание данной технической спецификации, но будут рассмотрены в следующих отчетах: «Оценка стандартов по безопасности и конфиденциальности» и «Службы обеспечения конфиденциальности и безопасности» (см. подраздел 2.2 «Контекст для анализа требований к конфиденциальности и безопасности»).

Требование конфиденциальности 12 канадской медицинской организации Infoway

Связывание директив согласия с ПМД в системах инфоструктуры EHR

Если наличие согласия требуется по закону, каждый раз при получении, хранении, обработке или передаче ПМД инфоструктура EHR должна быть способна:

a) поддерживать связь между данными и директивами согласия, в соответствии с которыми данные могут использоваться или разглашаться;

b) обрабатывать эти директивы согласия перед передачей связанных данных и блокировать передачу в случае, если она противоречит директиве, а также в случае, если никаких исключений для такого типа разглашения не указано в законе;

c) уведомлять инициатора запроса каждый раз при блокировке данных, согласно изложенному в перечислении b).

Обоснование — Это позволит организациям, подключающимся к инфоструктуре EHR или размечающим компоненты инфоструктуры EHR, применять директивы согласия пациента/лица в пределах их юрисдикции, а также в других юрисдикциях. Инфоструктуре EHR и системам, подключаемым к инфоструктуре EHR, будет также требоваться последовательное представление директив согласия и директив маскирования/безопасного хранения для поддержания требований интероперабельности в пределах юрисдикций и прежде всего между этими юрисдикциями.

Великобритания

Требование 3.2.5 Управления информацией Великобритании

Система должна гарантировать, что пользователь, который запрашивает доступ к конфиденциальным персональным данным, доступным в CRS NHS, сначала будет уведомлен о статусе согласия на обмен информации CRS NHS пациента, о дате последнего решения о согласии и о содержании решения о согласии пациента. PDS должен запрашиваться для такой информации, а не для локально хранимой информации.

Требование 3.16.10 Управления информацией Великобритании

Доступ из систем социальной помощи

Перед попыткой внести вклад в краткую медицинскую карту (путем отправки информации на PSIS) системы должны установить (с помощью интерфейса службы контроля доступа spine), что клиенты не возражают против создания краткой медицинской карты.

Требование 3.16.11 Управления информацией Великобритании

Доступ из систем социальной помощи

Перед отправкой любой информации из любых учреждений социальной помощи в информационные службы NHS (например, отправка сообщений CAF в PSIS) система должна обеспечить получение явно выраженного согласия от клиента. Ожидается, что механизм блокирования (см 3.5 и ссылки) будет использоваться для управления данным согласием: оценки, которые были заблокированы и защищены, не могут быть отправлены PSIS, в то время как оценки, которые заблокированы, могут быть отправлены, но не будут доступны для обычного просмотра остальным.

В.2.4 Игнорирование согласия в случае чрезвычайных обстоятельств

США

CCHIT IFR.02

Разрешает авторизованным пользователям (имеющим допуск при чрезвычайных обстоятельствах) осуществлять доступ к электронным медицинским данным в случае чрезвычайных обстоятельств.

Великобритания

Требование 3.2.6 Управления информацией Великобритании

Система должна гарантировать, что пользователь, который запрашивает доступ к конфиденциальным персональным данным, которые доступны в CRS NHS и относятся к пациентам, выразившим «явное несогласие», сначала будет уведомлен о последствиях перед выводом таких данных. Система должна гарантировать, что пользователь зарегистрировал подтверждение того, что данное уведомление было принято к сведению перед выводом данных. В таких обстоятельствах должны соблюдаться рекомендации, изложенные в NPFIT-FNT-K-IG-0114 DES — Проектирование диалога игнорирования несогласия.

В.2.5 Регистрация в журнале игнорирования согласия

Канада

Требование конфиденциальности 13 канадской медицинской организации Infoway

Регистрация игнорирования согласия

Инфоструктура EHR должна быть способна:

a) заносить в журнал случаи, при которых обработка директив согласия (см. требование конфиденциальности 12, перечисление b) запрещает передачу данных;

b) заносить в журнал идентификационные данные каждого пользователя, который игнорирует директивы согласия пациента/лица, причину игнорирования согласия, а также дату и время, в которое согласие было проигнорировано;

c) оповещать лицо, ответственное за обеспечение соблюдения конфиденциальности в организации, где работает пользователь, осуществляющий доступ, а также в организации, в которой проводился сбор информации, о том, что согласие было проигнорировано.

Обоснование — Так как некоторые законы о защите медицинских данных, например, *закон Онтарио о защите персональных медицинских данных*, разрешают осуществлять как маскировку, так и демаскировку, а также уведомлять третьих лиц о существующих маскировках, системы EHRi и POS, подключенные к инфоструктуре EHR, должны вести слежку путем занесения в журнал аудита идентификационных данных каждого, кто демаскирует или снимает блокировку с карт (см. требование безопасности 38 и требование безопасности 43).

Кроме того, некоторые законодательные акты о защите медицинских данных требуют, чтобы хранители медицинской информации уведомляли пациента/лицо о том, что его или ее информация украдена, утеряна или доступ к ней был осуществлен посторонним лицом. Уведомление о том, что директива согласия лица была проигнорирована, окажет значительную помощь лицу (лицам), ответственным за обеспечение соответствия организации требованиям конфиденциальности, в определении того, когда были осуществлены потенциальный «несанкционированный» доступ или разглашение ПМД. Игнорирование директив согласия пациента/лица должно контролироваться как в организации, в которой осуществлялся сбор ПМД, так и в организации, из которой будет осуществлен доступ к информации.

Поскольку журналы сами по себе будут содержать конфиденциальную информацию, они должны иметь защиту и исключать несанкционированный доступ. Требования к их безопасности описаны в требовании безопасности 50 (обеспечение доступа к журналам аудита инфоструктуры EHR) и требовании безопасности 51 (исключение несанкционированного доступа к журналам аудита инфоструктуры EHR).

Помимо регистрации случаев игнорирования директив согласия пациента/лица (см. перечисление b) и уведомления ответственных лиц о том, что директива согласия лица была проигнорирована (см. перечисление c), существует также связанное требование об уведомлении пациентов/лиц о несанкционированном доступе (см. требование конфиденциальности 20, приведенное в разделе 5).

Великобритания

Требование 3.2.7 Управления информацией Великобритании

Система должна гарантировать, что в случае вывода данных при обстоятельствах, описанных в требовании 3.2.6, это событие будет отражено в аудиторском следе с указанием следующих данных:

- идентификационных данных пользователя (включая идентификацию ролевого профиля);
- идентификационных данных пациента;
- даты и времени осуществления доступа;
- цели (целей) доступа.

В.2.6 Маскирование данных

Великобритания

Требование 3.5.1 Управления информацией Великобритании

Запечатанный конверт

В настоящее время разрабатываются средства, позволяющие пациентам принимать решения о доступности информации о них. Согласно описанию в Гарантии медицинской карты в будущем пациенты смогут просить, чтобы отдельные части их карт были скрыты от общего обзора, и при определенных обстоятельствах врач сможет скрыть определенные типы информации от пациента.

Блокирование поддерживается в Краткой истории болезни (SCR) от Spine выпуска 2008-А, а системам, взаимодействующим с Краткой историей болезни, теперь требуется поддерживать блокирование (по крайней мере с точки зрения их взаимодействия с SCR).

Дальнейшие подробности и рекомендации для поставщиков доступны в NPFIT-FNT-K-REQDEL-0142 Требования поставщика о запечатанных конвертах и сопутствующей таблице, описывающей применимость этих требований в различных контекстах.

Требование 3.16.12 Управления информацией Великобритании

Доступ из систем социальной помощи

При осуществлении доступа к данным от PSIS системы социальной помощи должны отбирать доступные данные и позволять пользователям осуществлять доступ только к данным, касающимся социальной помощи.

В.2.7 Согласие, данное заменяющим ответственным лицом

Канада

Требование конфиденциальности 15 канадской медицинской организации Infoway

Запись идентификационных данных заменяющих ответственных лиц

В случае необходимости выполнения данных действий в силу закона системы EHRi и POS, подключенные к инфоструктуре EHR, должны иметь возможность отображения того, что согласие дано заменяющим ответственным лицом от имени пациента/лица (например, согласие дано уполномоченным представителем), а также идентифицировать это заменяющее ответственное лицо и его отношение к пациенту/лицу.

Обоснование — Согласие может быть дано не только пациентом/лицом, но и уполномоченным представителем (например, законным опекуном, заменяющим ответственным лицом или лицом, имеющим доверенность). Создание возможности согласия и предоставление заменяющего ответственного лица являются двумя самыми сложными проблемами защиты данных. Провинциальные и территориальные законы регулируют эту деятельность.

Определение заменяющего ответственного лица пациента, как правило, является процессом распределения по степени важности, при котором, в случае если ни один человек, соответствующий первой роли/родству в списке (например, супруг или опекун) не может быть найден, то хранитель должен попытаться найти следующее потенциальное заменяющее ответственное лицо в процессе распределения по степени важности (например, брата).

Когда подходящее заменяющее ответственное лицо найдено, хранитель должен зарегистрировать его отношение к пациенту/лицу для того, чтобы обеспечить возможность проведения аудита, подтверждения или переоценки осуществленного выбора.

В.2.8 Оповещение пациентов об изменении согласия

Великобритания

Требование 3.16.9 Управления информацией Великобритании

Доступ из систем социальной помощи

Система должна предоставлять средства, позволяющие организации, использующей систему, уведомлять клиентов об изменениях их статуса согласия и/или при его регистрации или отмене для того, чтобы убедиться, что такие изменения были внесены надлежащим образом в ответ на пожелания клиента. Это может быть выполнено в форме отчета, который доступен системным администраторам, или местных сообщений, отправленных определенным администраторам.

В.3 Ограничение использования и разглашения

Канада

Требование конфиденциальности 18 канадской медицинской организации Infoway

Ограничение использования и разглашения персональных медицинских данных для различных целей

Организации, подключающиеся к инфоструктуре EHR, и организации, размещающие компоненты инфоструктуры EHR, должны использовать или раскрывать ПМД только с целью осуществления задач, согласующихся

с теми, для которых они были собраны, за исключением случаев, когда это осуществляется с согласия пациента/лица либо разрешено или требуется по закону.

Обоснование — Закон провинции Альберта о защите медицинской информации, закон провинций Манитоба и Онтарио о защите персональных медицинских данных, а также закон провинции Онтарио о персональной медицинской информации требуют, чтобы хранители ПМД собирали, использовали и разглашали только тот объем ПМД, который оправданно необходим для осуществления установленных задач. Более подробная информация приведена ниже в «Обязанностях по сбору, использованию и разглашению в условиях ограничения».

Кроме того, это требование является стандартным и относится к принципам честного использования данных, а в учреждениях, где были введены законодательные акты о защите медицинских данных, не препятствует хранителям информации обеспечивать медицинское обслуживание. Эти законодательные положения, как правило, разрешают или требуют несколько использований или разглашений ПМД, относящихся к обеспечению медицинского обслуживания, поддержке работы системы здравоохранения или обеспечению общественного здравоохранения; такие законодательные положения могут различаться в зависимости от юрисдикции.

Великобритания

Требование 3.4.1 Управления информацией Великобритании

Родство, признанное законом (LR)

Системы и услуги, введенные в рамках Национальной программы по информационным технологиям (National Programme for Information Technology, NPfIT), предоставляемые объединением здравоохранения [Connecting for Health (CFH)] Национальной службы здравоохранения Великобритании, будут безопасно обрабатывать персональные данные о пациентах, учитывая конфиденциальность пациента. Среди элементов управления существует требование, что только те пользователи, которые имеют «признанное законом родство» (LR) с пациентом, будут иметь доступ к личной информации о нем.

Только те пользователи, которые учувствуют в предоставлении медицинского обслуживания и поддержке пациента, обладают выраженным согласием пациента на доступ к его данным. Без такого согласия обычный доступ к данным не может быть осуществлен.

Системы должны гарантировать, что доступ к определенным картам пациентов контролируется должным образом. Например, при использовании GP-системы, любые карты пациентов, более не зарегистрированных в работе, не должны быть доступны в обычном порядке пользователям системы.

Требование 3.11.7 Управления информацией Великобритании

Поставщик должен показать, что он ограничил идентифицируемые данные пациентов, передаваемые на портативные носители, до минимума, необходимого для соответствующей службы.

В.4 Доступ пациента к персональной информации и исправление неточных данных

Бразилия

NGS1.04.08

Доступ пациентов к RES

Необходимо убедиться, что пациент может осуществлять доступ ко всей его/ее личной и клинической информации, хранящейся в EHR. Если EHR не позволяет пациенту осуществлять прямой доступ к EHR, то должна использоваться роль пользователя, которая позволяет осуществлять действия от имени пациента.

Пациент должен иметь возможность забрать с собой информацию в печатном или электронном формате. Система должна быть обеспечена интерфейсом для печати заявления пользователя о том, что он или она получают информацию.

В случаях когда пациент имеет прямой доступ к информации или когда другое лицо имеет прямой доступ к информации пациента, любой экспорт данных и печать заявления пациента должны быть записаны с указанием как минимум следующей информации:

- пользователь, выполняющий данное действие;
- полное имя пациента;
- место и время действия.

HL7 ERH-S FM IN1.4.

Канада

Требование конфиденциальности 25 канадской медицинской организации Infoway

Исправление неточной и неполной информации

Организации, подключающиеся к инфоструктуре EHR, и организации, размещающие компоненты инфоструктуры EHR, должны:

a) исправлять ПМД, когда пациент/лицо успешно подтверждает неточность или неполноту такой информации;

b) уведомлять пользователей инфоструктуры EHR о том, что доступ к рассматриваемой информации был осуществлен, и информация была изменена в тех случаях, когда можно обоснованно ожидать, что изменение информации окажет влияние на текущее лечение пациента/лица;

c) записывать суть нерешенного спора в случаях, когда организация не согласна с тем, что пациент/лицо сочли неполным или неточным в ходе своей оценки;
d) сообщать о факте наличия нерешенного спора пользователям инфоструктуры EHR, осуществляющим доступ к рассматриваемой информации.
Обоснование — Решения, принятые уполномоченными лицами по информации и конфиденциальности (или их заместителями по всей Канаде), привели к результатам в правовой практике, подчеркивающим, что только фактические ошибки могут быть исправлены в соответствии с фактами, например, дата рождения. Спорными вопросами, касающимися заключения специалиста, включая диагноз, поставленный медицинским работником, являются именно те, которые пациент/лицо хочет оспорить. Вопросы, касающиеся исправлений, удалений или дополнений, являются особенно актуальными, если информация может привести к изменениям в лечении лица или в решениях, принятых по отношению к нему или к ней. В зависимости от характера оспариваемой информации коррекция может включать исправление, удаление или дополнение информации. Некоторые исправления, удаления или изменения могут иметь особое значение для текущего медицинского облуживания пациента/лица и должны получить огласку должным образом. К счастью, разработанная система электронного учета здоровья будет автоматически распределять наиболее актуальную информацию в случаях, когда это будет необходимо для осуществления официально утвержденных задач.

Великобритания

Требование 3.18.1 Управления информацией Великобритании
Поставщик должен гарантировать, что система, хранящая личные данные, была способна отвечать на запросы субъекта на доступ в соответствии с Законом о защите данных 1998 г.
Требование 3.18.2 Управления информацией Великобритании
Поставщик должен гарантировать, что система позволяет авторизованным пользователям отбирать из электронных карт пациента данные, просмотр которых может быть нежелателен для пациента, и/или информацию о третьих лицах перед отправкой ответа на запрос субъекта.
Требование 3.18.3 Управления информацией Великобритании
Поставщик должен гарантировать, что система позволяет пользователю регистрировать запрос субъекта на доступ.
Требование 3.18.4 Управления информацией Великобритании
Поставщик должен гарантировать, что система предусматривает, что данные о запросе субъекта на доступ, которые могут быть записаны, включают как минимум дату получения запроса, идентификационные данные субъекта, идентификационные данные лица, составляющего запрос субъекта на доступ, идентификационные данные пользователя и организации, ответственной за ответ на запрос, идентификационные данные лечащего врача, давшего консультацию перед выдачей персональных данных, информацию о том, был ли запрос отклонен, причину отказа в свободной форме, конфиденциальную причину отказа и дату ответа на запрос, а также любую другую информацию, которую ответственное лицо должно соответствующим образом указать.
Требование 3.18.5 Управления информацией Великобритании
В случаях, когда запрос субъекта на доступ отклонен, подрядчик должен гарантировать, что сервис требует выбрать как минимум одну причину отказа из заранее установленного списка, который будет частью национального стандарта (как это время от времени требует уполномоченное лицо).
Требование 3.18.6 Управления информацией Великобритании
Система должна применять признанное законом родство (см. требование 3.4.1) или аналогичные средства контроля доступа для управления доступом к функциональным средствам, описанным в данном разделе.
Требование 3.18.7 Управления информацией Великобритании
Система должна предоставлять функциональные средства для мониторинга запросов SAR в ходе работы и для составления отчетов о выполняемых задачах.

Российская Федерация

Закон РФ 2011-11-21 N323, статья 22 Информация о состоянии здоровья
Пациент имеет право получить доступ к имеющейся в медицинской организации информации о состоянии своего здоровья, в том числе к сведениям о результатах медицинского обследования, о диагнозе и т. д. Все данные должны быть предоставлены в доступной форме. Эти данные должны быть предоставлены пациенту его/ее лечащим врачом или другим медицинским работником, который принимал непосредственное участие в лечении этого пациента.
Информация о состоянии здоровья не может быть предоставлена пациенту против его воли. Пациент или его законный представитель имеет право непосредственно ознакомиться с медицинской документацией, отражающей состояние его здоровья, и получить на основании такой документации консультации у других специалистов.
Пациент либо его законный представитель имеет право на основании письменного заявления получать отражающие состояние здоровья медицинские документы, их копии и выписки из медицинских документов.

В.5 Точность данных

Канада

Требование конфиденциальности 22 канадской медицинской организации Infoway

Точность

Системы EHRi и POS, подключенные к инфоструктуре EHR, организации, подключающиеся к инфоструктуре EHR, и организации, размещающие компоненты инфоструктуры EHR, должны предпринять разумные шаги или меры для того, чтобы:

a) гарантировать полноту, точность и актуальность персональных медицинских данных в соответствии с необходимыми условиями для осуществления задач, при которых используются данные, включая разглашение ПМД третьим лицам, и

b) точно идентифицировать пациента/лицо при осуществлении доступа или модификации его/ее ПМД.

Обоснование — Среда электронных медицинских карт должна способствовать достижению более высокого качества медицинских карт путем установки аппаратного контроля ввода данных и облегчения обновления даже самых основных демографических данных и сведений о местонахождении любого пациента/лица.

Кроме того, точная идентификация пациента/лица перед осуществлением доступа или изменением их ПМД крайне важна для обеспечения безопасности пациентов и для ряда других причин, в том числе для исправности системы EHR в целом.

В.6 Идентификация и аутентификация пользователей

В.6.1 Идентификация пользователя

Бразилия

NGS1.02.01

Идентификация (и аутентификация) пользователей

Все пользователи должны быть идентифицированы (и аутентифицированы) перед получением доступа к любым данным EHR, включая случаи, когда подключение к сети отсутствует: например, при использовании мобильных устройств.

HL7 ERH-S FM IN1.1; ABNTNBR ИСО/МЭК 27001:2005, A.11.5.2.

США

CCHIT IFR.01

Присвоение уникального имени и/или номера для идентификации и отслеживания идентификационной информации пользователя

Канада

Требование безопасности 55 канадской медицинской организации Infoway

Присвоение идентификаторов пользователю

Все организации, подключающиеся к инфоструктуре EHR, должны гарантировать, что пользователям систем POS, подключенных к инфоструктуре EHR, присвоены идентификаторы (идентификационные номера пользователя), которые в сочетании с другими идентификаторами (например, идентификатор учреждения, юрисдикции и т. д.) однозначно устанавливают личность пользователя в пределах инфоструктуры EHR. Системы POS должны поддерживать однозначную идентификацию пользователей.

Обоснование — Данное требование облегчает проведение общесистемного аудита и обеспечение надежной защиты данных в линии передачи.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)

Все пользователи должны быть идентифицированы.

В.6.2 Идентификационные номера пользователей

США

CCHIT SC 03.08

Аутентификация

Система должна поддерживать имена пользователей без учета регистра, которые содержат типовые буквенно-числовые символы для обеспечения выполнения ИСО-646/ECMA-6 (также известного как US ASCII, или Американский стандартный код для обмена информацией).

ИСО/МЭК 15408, *CCSFR: FMT_MTD;*

HIPAA: 164.312(a) (2)(i).

В.6.3 Аутентификация пользователя

Бразилия

NGS1.02.01

Идентификация и аутентификация пользователя

Все пользователи должны быть (идентифицированы и) аутентифицированы перед получением доступа к любым данным EHR, включая случаи, когда подключение к сети отсутствует: например, при использовании мобильных устройств.

HL7 ERH-S FM IN1.1; ABNTNBR ИСО/МЭК 27001:2005, A.11.5.2.

США

CCHIT SC 03.01

Система должна проводить аутентификацию пользователя перед предоставлением доступа к защищенным ресурсам (например, ПМД), включая случаи, когда подключение к сети отсутствует: например, при использовании мобильных устройств.

Канада: Alberta 1.1 (Альберта 1.1);

ИСО/МЭК 15408, *CC SFR: FIA_UAU, FIA_UID;*

NIST SP 800-53: IA-2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ;

HIPAA: 164.312(d).

CCHIT IFR.09

Необходимо убедиться в том, что лицо или организация, запрашивающие доступ к электронной медицинской информации через сеть, имеют право на доступ к такой информации в соответствии со стандартом, указанным в таблице 2B, строка 5.

Таблица 2B строка 5. Аутентификация между предприятиями: использование безопасных операций между предприятиями, которые содержат достаточную идентификационную информацию, например, таких, при которых получатель может принимать решения в системе контроля доступа и составлять детальные и точные журналы аудита [например, аутентификация между предприятиями IHE (XUA) с подтверждением идентификационных данных на языке SAML].

Канада

Требование безопасности 71 канадской медицинской организации Infoway

Надежная аутентификация пользователя

Инфоструктура EHR и все системы POS, подключенные к инфоструктуре EHR, должны надежно аутентифицировать пользователей.

Обоснование — Неконтролируемый доступ пользователей является частой причиной нарушения безопасности. Кроме того, для поддержания некоторого уровня однородности устойчивости аутентификации, скорее всего, будет необходима поддержка межюрисдикционной совместимости.

Необходимо отметить, что это требование, скорее всего, потребует реализации надежных технологий аутентификации, включающих:

a) цифровые сертификаты;

b) технику биометрической идентификации;

c) смарт-карты или другие аппаратные ключи безопасности; или

d) безопасные, основанные на стандарте и надежные схемы паролей.

Предполагается, что системы EHRi и POS, подключенные к инфоструктуре EHR, будут работать вместе для выполнения задачи по аутентификации пользователей, имеющих доступ к инфоструктуре EHR; т. е. пользователи не должны быть аутентифицированы дважды.

Великобритания

Требование 3.1.2 Управления информацией Великобритании

Система должна гарантировать, что все пользователи, которые имеют доступ к персональным данным или конфиденциальным персональным данным пациентов, полученным из хранящихся в или подлежащим хранению в CRS NHS, безопасно аутентифицированы с помощью стандартных смарт-карт или идентификационных данных, предоставленных NASP.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)

Все пользователи должны быть аутентифицированы перед осуществлением доступа к:

- операционной системе;
- средствам обеспечения безопасности;
- журналам аудита.

B.6.4 Аутентификация системой и аутентификация сетевого узла

Бразилия

NGS1.06.02

Контроль доступа от клиента к системе

При осуществлении дистанционного доступа S-RES доступ к системе ограничен и доступен только клиентам, имеющим предварительное разрешение. Такой контроль доступа может осуществляться, к примеру, через IP-адрес клиента.

ABNT NBR ИСО/МЭК 27001:2005, A.11.4.2.

NGS1.06.05

Контроль доступа между компонентами

В системе EHR, состоящей из нескольких распределенных компонентов (т. е. размещенных на разных компьютерах), в процессе коммуникации между этими компонентами (например, база данных) доступ к компоненту должен быть ограничен и доступен только партнерам (компонентам) с предварительным разрешением.

ABNT NBR ИСО/МЭК 27001:2005, A.10.9.2.

США

CCHIT SC 06.12

Технические службы

Убедитесь в том, что лицо или организация, запрашивающая доступ к электронной медицинской информации через сеть, имеет право на доступ к такой информации в соответствии со стандартом, указанным в таблице 2B, строке 5.

Таблица 2B строка 5. Аутентификация между предприятиями: Использование безопасных операций между предприятиями, которые содержат достаточную идентификационную информацию, например, таких, при которых получатель может принимать решения в системе контроля доступа и составлять детальные и точные журналы аудита [например, аутентификация между предприятиями IHE (XUA) с подтверждением идентификационных данных на языке SAML].

CCHIT SC 06.05

Технические службы

Система должна обеспечивать аутентичность удаленных узлов (общую аутентификацию узлов) при обмене защищенными медицинскими данными по сети Интернет или другой известной открытой сети посредством открытых протоколов (например, TLS, SSL, IPSec, XML Sig, S/MIME).

ИСО/МЭК 15408, *CC SFR: FPT_RCV; HITSP T17;*

HIPAA: 164.312(d); 164.312(c)(1).

Канада

Требование безопасности 65 канадской медицинской организации Infoway

Аутентификация доступа к сети инфоструктуры EHR

Организации, размещающие компоненты инфоструктуры EHR, должны гарантировать, что все подключения инфоструктуры EHR к удаленным серверам и приложениям аутентифицированы. Данное требование относится также к подключениям через сеть Интернет.

Обоснование — Данное требование помогает гарантировать, что приложения, содержащие ПМД, не повреждены в результате нелегального проникновения на удаленные серверы и/или в приложения.

Великобритания

Требование 3.7.2 Управления информацией Великобритании

Поставщик должен гарантировать, что все подключения к удаленным серверам и приложениям аутентифицированы. Данное требование относится также к подключениям через сеть Интернет.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)

Все узлы сети должны быть идентифицированы с помощью логических имен (адресов, номеров).

B.6.5 Методы аутентификации

Бразилия

NGS1.02.02

Метод аутентификации

Используйте как минимум один из следующих методов аутентификации:

- имя пользователя и пароль;
- цифровой сертификат;
- одноразовый пароль (OTP) и/или
- технику биометрической идентификации.

Примечание — Любые другие методы аутентификации должны быть утверждены заранее.

HL7ERH-SFMIN1.1 ABNTNBR ИСО/МЭК 27001:2005, A.11.5.1.

NGS2.03.02

Отказоустойчивость аутентификации

Условие — Системы EHR, использующие цифровые сертификаты для аутентификации.

Аутентификация, проведенная с помощью цифрового сертификата, должна создавать доказательство для обеспечения отказоустойчивости аутентификации. Доказательство должно храниться в журналах безопасности системы в форматах, соответствующих стандарту CMS [RFC 3852] или XMLDSIG [RFC 3275]. Все элементы, необходимые для проверки аутентификации (информация о корневых сертификатах, цепочке сертификатов, сертификатах подписывающего лица и информация об аннулировании), должны быть агрегированы в EHR.

NGS2.03.03

Типы пользователей, использующих цифровые сертификаты для аутентификации

Условие — Системы EHR, использующие цифровые сертификаты для аутентификации.

Все пользователи, использующие цифровые подписи, должны быть аутентифицированы с помощью своих цифровых сертификатов Инфраструктуры открытых ключей Бразилии.

NGS2.03.04

Утверждение Инфраструктуры открытых ключей Бразилии (особое для Бразилии)

Условие — Системы EHR, использующие цифровые сертификаты для аутентификации.

Компоненты EHR, использующие цифровые сертификаты для аутентификации, должны быть утверждены Инфраструктурой открытых ключей Бразилии.

NGS2.03.01

Проверка назначения цифрового сертификата для аутентификации

Условие — Системы EHR, использующие цифровые сертификаты для аутентификации.

Перед аутентификацией проверьте, имеет ли используемый цифровой сертификат функциональное назначение аутентификации (аутентификация клиента).

Великобритания

Требование 3.1.8 Управления информацией Великобритании (требование Великобритании по использованию смарт-карт для конкретного случая)

Система должна предоставлять механизм для привязки смарт-карты пользователя к записи пользователя в пределах системы. Такой механизм как минимум должен включать идентификатор пользователя SDS, однако при необходимости может включать и другие идентификаторы (например, идентификаторы ролевого профиля). Присвоение идентификатора SDS должно осуществляться через системную функцию ограниченного доступа и должно быть выполнено программным путем (см. псевдокод ниже). Все подобные присвоения должны быть зарегистрированы в соответствующем аудиторском следе. Доступ к удалению или изменению таких присвоений подобным образом должен осуществляться только с помощью функции ограниченного доступа, а все записи об изменениях должны быть занесены в соответствующий аудиторский след.

Исполнители:

- оператор — лицо, использующее систему, которое предоставляет новую смарт-карту пользователю системы;
- пользователь — лицо, чья (новая) смарт-карта привязана к его записи пользователя в системе.

Предварительное условие — Оператор должен иметь доступ к защищенной функции присвоения смарт-карт. Он может аутентифицироваться либо с помощью SSB, либо локально (т. е. введя имя пользователя и пароль в локальную систему).

НАЧАЛО

ЕСЛИ оператор аутентифицирован сервисом SSB, ТО НАЧНИТЕ

Запросите оператора удалить его смарт-карты

Позвольте оператору продолжить использование системы (т. е. не выводите оператора из системы, потому что он удалил свои смарт-карты или потому что было получено сообщение слушателя событий в связи с удалением данной смарт-карты)

КОНЕЦ

Запросите введение смарт-карты пользователя

Пользователь аутентифицируется самостоятельно (ввод PIN-кода)

ЕСЛИ аутентификация прошла успешно, ТО НАЧНИТЕ

Система получает подтверждения на языке SAML и программным путем выделяет идентификатор пользователя SDS и любые необходимые идентификаторы ролевого профиля (RoleProfileIDs)

При необходимости оператор должен сохранить любые необходимые идентификаторы ролевого профиля (RoleProfileIDs)

Система хранит ID пользователя SDS и любые необходимые идентификаторы ролевого профиля (RoleProfileIDs)

КОНЕЦ

ЕСЛИ оператор был аутентифицирован сервисом SSB, ТО НАЧНИТЕ

Запросите оператора ввести свои смарт-карты и пройти повторную аутентификацию

Позвольте оператору продолжить использование системы

КОНЕЦ

Требование 3.1.3 Управления информацией Великобритании (требование Великобритании по использованию смарт-карт для конкретного случая)

Система также должна поддерживать вход в систему, независимый от сервиса SSB, если SSB недоступен, кроме случаев, когда:

- не требуется извлечения роли пользователя и других атрибутов управления доступом из SDS;
- надежность аутентификации может быть ниже, чем та, что используется для входа в систему из SSB;
- пользователь не получит право доступа к системам и данным CRS NHS, пока не пройдет повторную аутентификацию в соответствии с описанием в требовании 3.1.4; однако доступ к данным, содержащимся в локальной системе, может быть осуществлен в процессе использования локальной аутентификации, в случаях когда SSB недоступен;
- в случаях когда система поддерживает понятие «конфиденциальные персональные данные» (или аналогичные термины), локальные средства управления доступом на основе ролей (RBAC) должны включать в себя ограниченный доступ к таким данным.

Во избежание неоднозначности толкования использование входа в систему, независимого от сервиса SSB, в данном требовании предполагается только в случаях, при которых сервис SSB временно недоступен.

Требование 3.1.4 Управления информацией Великобритании (требование Великобритании по использованию смарт-карт для конкретного случая)

В случаях когда пользователь осуществил вход в систему независимо от сервиса SSB, в соответствии с описанием в требовании 3.1.3 система должна предотвратить несанкционированный доступ к системам и данным CRS NHS (несмотря на это, доступ к данным, содержащимся в локальных системах, может быть осуществлен в процессе использования локальной аутентификации, когда SSB недоступен). В таких случаях система может либо активировать вход в CRS NHS и применить средства управления доступом CRS NHS при попытке пользователя получить доступ у системам CRS NHS или предоставить вызов функции входа в CRS NHS из системы. То есть пользователю не требуется выходить из системы для аутентификации SSB и осуществлять повторный вход до получения доступа к CRS NHS. После того как пользователь успешно завершил вход в CRS NHS, он должен оставаться аутентифицированным для CRS NHS в течение всего локального сеанса, при этом соответствуя времени ожидания сеанса Spine, времени ожидания активности и требованиям удаления смарт-карты.

Единственным исключением к данному требованию является случай, когда взаимодействия, инициированные системой, могут извлекать данные PDS с помощью средства извлечения PDS или простых сообщений о трассировке PDS. Системы не должны вводить какие-либо данные в SSB без аутентификации.

Требование 3.1.9 Управления информацией Великобритании (требование Великобритании по использованию смарт-карт для конкретного случая)

Пользователи, чьи смарт-карты не зарегистрированы в системе (см. предыдущее требование), могут использовать только локальную аутентификацию и вследствие этого не получат доступ к функциям системы, которые требуют использования смарт-карты.

Требование 3.1.10 Управления информацией Великобритании (требование Великобритании по использованию смарт-карт для конкретного случая)

Периодически приложение должно проверять наличие локальных разрешений для того, чтобы гарантировать наличие аутентифицированной смарт-карты, за исключением случаев, когда приложение создает действующее исключение, позволяющее удалить смарт-карту для получения новой.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)

Имя пользователя и пароль

В.6.6 Защита профилей пользователя, пароли и другие аутентификационные маркеры

Бразилия

NGS1.02.03

Защита параметров аутентификации

Все данные или параметры, использованные в процессе аутентификации пользователя, должны храниться или передаваться безопасным способом. Например, путем хранения только хэш-кодов пароля пользователя и обеспечения ограниченного доступа к месту хранения. Должны использоваться только абсолютно безопасные алгоритмы, например SHA-1, SHA-2 или последующие алгоритмы, и/или криптографическая защита с помощью стандарта тройного шифрования данных (3DES), продвинутого стандарта шифрования (AES) и их преемников.

Примечание — При применении технологий, которые используют начальные числа для создания кода, начальное число должно быть защищено от несанкционированного доступа и изменения.

США

CCHIT SC 03.11

Аутентификация

При использовании паролей система должна поддерживать возможность защиты паролей во время передачи или хранения посредством использования криптографического хэширования с помощью SHA1, SHA 256 или их преемников и/или криптографической защиты с помощью Стандарта тройного шифрования данных (3DES), Продвинутого стандарта шифрования (AES) и их преемников.

Канада: Онтарио 5.3.12.a (управление доступом к системе);

ИСО/МЭК 15408, CCSFR: FCS_CKM;

NIST SP 800-53: SC-12 СОЗДАНИЕ И УПРАВЛЕНИЕ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ;

HIPAA: 164.312(e)(1); 164.308(a)(5)(ii)(D).

FIPS PUB 197

FIPS PUB 140-2

CCHIT SC 06.02

Технические службы

При использовании паролей система не должна отображать пароль во время его ввода.

ИСО/МЭК 15408, CC SFR: FPT_ITC;

ИСО/МЭК 27002:2005, 9.2.3;
HIPAA 164.312(a) (1).

Великобритания

Требование 3.3.8 Управления информацией Великобритании

Система должна гарантировать, что при локальном хранении информация о профиле пользователя, которая поддерживает механизм RBAC, защищена от несанкционированного доступа (включая просмотр, изменение или удаление).

В.6.7 Пароли

Бразилия

NGS1.02.04

Качество пароля

Условие — Использование аутентификации на основе имени пользователя/пароля.

Используйте следующие средства управления безопасностью:

Качество пароля — Проверьте качество пароля сразу после его создания пользователем. Пароль должен состоять как минимум из восьми символов, по крайней мере один из которых должен быть не буквенным.

Частота изменения пароля — Система EHR должна включать в себя функциональные возможности, которые принуждают пользователя изменять пароль в соответствии с регулируемым максимальным периодом времени.

ABNT NBR ИСО/МЭК 27001:2005, А.11.5.3.

США

CCHIT SC 03.02

Аутентификация

При использовании паролей система должна поддерживать правила обеспечения надежности паролей, которые допускают использование минимального количества символов, и усложнения путем использования буквенных и цифровых символов.

Канада: Альберта 7.3.12 (безопасность);
Канада: Онтарио 5.3.12.b (управление доступом к системе);
ИСО/МЭК 15408, CC SFR: FIA_SOS, FIA_UAU, FIA_UID;
ASTM: E1987-98;
NIST SP 800-53: IA-2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ (надежность пароля не описана);
ИСО/МЭК 27002:2005, 9.3.1.d;
HIPAA: 164.

CCHIT SC 03.05

Аутентификация

При использовании паролей система должна предоставлять административную функцию, которая позволяет осуществлять сброс пароля.

ИСО/МЭК 15408, CC SFR: FMT_MTD;
ИСО/МЭК 27002:2005, 9.2.3.b, (9.3.1.f);
HIPAA: 164.312(d); 164.308(5) (ii) (D).

CCHIT SC 03.06

При использовании паролей учетные записи пользователей, которые были сброшены администратором, должны требовать изменения пароля пользователем при следующем успешном входе в систему.

ИСО/МЭК 15408, CC SFR: FMT_MTD;
ИСО/МЭК 27002:2005, 9.2.3.b, (9.3.1.f);
HIPAA: 164.312(d); 164.308(5) (ii) (D).

CCHIT SC 03.09

Аутентификация

При использовании паролей система должна позволять аутентифицированным пользователям изменять свои пароли в соответствии с правилами обеспечения надежности пароля (SC 03.02).

ИСО/МЭК 15408, CC SFR: FMT_MTD;
HIPAA: 164.308(a) (5) (ii) (D).

CCHIT SC 03.10

Аутентификация

При использовании паролей система должна учитывать регистр паролей, которые содержат типируемые буквенно-цифровые символы для обеспечения выполнения ИСО-646/ECMA-6 [также известного как US ASCII (американский стандартный код для обмена информацией)].

Канада: Онтарио 5.3.12 (b);
NIST SP 800-63;
HIPAA: 164.308(a) (5) (ii) (D).

Великобритания

Требование 3.15.2 Управления информацией Великобритании (требование Великобритании, относящееся к конкретному случаю)

Любая локальная аутентификация должна основываться на идентификационных данных пользователя, которые затем аутентифицируются по крайней мере путем использования отдельного пароля.

Требование 3.15.3 Управления информацией Великобритании (требование Великобритании, относящееся к конкретному случаю)

Управление паролем должно осуществляться в соответствии с рекомендациями в CESG Infosec, пояснительная записка № 26 службы информационной безопасности Группы безопасности электронных коммуникаций, предоставляемыми по запросу, направленному на электронную почту esp.ig@nhs.net.

Требование 3.15.5 Управления информацией Великобритании (требование Великобритании, относящееся к конкретному случаю)

Системы должны гарантировать, что пароли могут быть приведены в соответствие с политикой согласно определению в рекомендации: NPFIT-FNT-TO-IG-IGCOM-0066 Политика паролей однофакторной аутентификации.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)

Качество пароля — Пароль должен состоять из шести или более буквенно-цифровых символов.

В.6.8 Неудачные попытки входа

США

SC 03.04

Аутентификация

Система должна ввести ограничение (конфигурируемое) на количество последовательных неудачных попыток доступа пользователя. Система должна обеспечивать защиту от дальнейших, возможно злоумышленных, попыток аутентификации пользователя с помощью соответствующего механизма (например, блокировка учетной записи/узла до отмены администратором, блокировка учетной записи/узла на регулируемый период времени или задержка следующего приглашения на вход в систему в соответствии с настраиваемым алгоритмом задержки).

Канада. Онтарио 5.3.12.c (Управление доступом к системе);

ИСО/МЭК 15408, CC SFR: FIA_AFL, FMT_SAE;

NIST SP 800-53: AC-6 НЕУДАЧНЫЕ ПОПЫТКИ ДОСТУПА, AC-11 БЛОКИРОВКА СЕАНСА;

ИСО/МЭК 27002:2005, 9.3.1.e, 9.5.2.e;

HIPAA: 164.312(a)(1); 164.308(a)(5)(ii)C; 164.308(a)(6).

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)

Система должна ввести ограничение на количество последовательных неудачных попыток доступа пользователя к подсистеме безопасности.

В.6.9 Обратная связь с пользователем во время аутентификации

США

CCHIT SC 03.07

Аутентификация

Система должна предоставлять пользователю только ограниченный поток обратной информации в ходе аутентификации.

ИСО/МЭК 15408, *CC SFR: FIA_UAU;*

NIST SP 800-53: IA-6 ОБРАТНАЯ СВЯЗЬ ВО ВРЕМЯ АУТЕНТИФИКАЦИИ;

HIPAA: 164.312(d); 164.308(5) (ii) (D).

В.7 Управление привилегиями

В.7.1 Разрешение на доступ

Бразилия

NGS1.04.03

Управление пользователями

Обеспечьте возможность управления пользователями (создание, удаление и изменение), управления ролями (создание, удаление и изменение) и управления группами (создание, удаление и изменение).

NGS1.04.04

Роли, связанные с ИТ

Необходимо поддерживать функции, позволяющие осуществить как минимум следующие действия:

- аудиты журналов системных операций;
- установку системы;
- управление разрешениями;

- управление пользователями;
- создание и восстановление резервной копии.

NGS1.04.05

Установка контроля доступа

Следует обеспечить механизмы, необходимые для реализации политики управления доступом, с помощью установки профиля доступа, учитывающего роль пользователя, группы и операции, которые могут быть выполнены, включая различия между запросами и включениями/изменениями. Следует учитывать, что один пользователь может иметь несколько ролей.

HL7 ERH-S FM IN1.2;
ABNT NBR;
ИСО/МЭК 27001:2005, А.11.6;
ИСО 18308:2011(E) PRS3.3.

CCHIT SC 01.02

Контроль доступа

Система должна предоставлять авторизованным администраторам возможность назначать права и ограничения пользователям/группам.

Канада: Альберта 4.1.3 (EMR);
ИСО/МЭК 15408, CC SFR: FMT_MSA;
NIST SP 800-53: AC-56 LEAST PRIVILEGE; AC-5 SEPARATION F DUTIES
HIPAA: 164.312(a)(1); 164.308(A)(3)(1); HITSP/TP20.

CCHIT SC 01.03

Контроль доступа

Система должна быть способна связывать разрешения с пользователем посредством одного или нескольких средств управления: 1) на основе пользователя (право доступа дается каждому пользователю); 2) на основе ролей (пользователи сгруппированы, и право доступа предоставляется группе); 3) на основе контекста [на основе ролей с предоставлением или ограничением дополнительного права доступа в зависимости от контекста транзакции, например, времени суток (time-of-day), местоположения рабочей станции (workstation-location), режима чрезвычайной ситуации (emergency-mode) и т. д.].

Канада. Онтарио 5.3.12.e (управление доступом к системе);

ИСО/МЭК 15408, *CC SFR: FDP_ACC, FMT_MSA*;
ASTM: E1985-98;
NIST SP 800-53: AC-3 ACCESS AND INFORMATION FLOW CONTROL; SC-3 SECURITY FUNCTION ИСОLATION
HIPAA: 164.312(a)(1); 164.308(A)(3)(1);
HITSP/TP20.

Канада

Требование безопасности 58 канадской медицинской организации Infoway

Предоставление доступа пользователям в соответствии с их ролями.

EHRi и все системы POS, подключенные к инфоструктуре EHR, должны поддерживать ролевую модель управления доступом (RBAC), имеющую возможность сопоставления каждого пользователя с одной или несколькими ролями и каждую роль с одной или несколькими системными функциями.

Обоснование — На практике пользователи систем POS, подключенных к инфоструктуре EHR (их могут быть тысячи), не могут быть отдельно сопоставлены с функциями системы после регистрации пользователя с целью контроля объема их прав доступа. Выполнение этого сопоставления для каждого отдельного пользователя является очень сложным и подвержено возникновению множества ошибок. Скорее, пользователи должны быть сопоставлены с ролью, а затем роли сопоставлены с функциями системы.

Существуют значительные проблемы, связанные с использованием RBAC для поддержки совместимого EHR, которые должны быть устранены перед тем, как инфоструктура EHR сможет полностью и эффективно использовать RBAC. В приложении А, подраздел «Последствия нарушения конфиденциальности и безопасности, связанные с исполнителями», приведена сводка таких проблем.

Требование безопасности 60 канадской медицинской организации Infoway

Предоставление доступа пользователям в рабочих группах

EHRi и все системы POS, подключенные к инфоструктуре EHR, должны быть способны закреплять пользователей за рабочей группой и предоставлять доступ к картам в соответствии с рабочей группой.

Обоснование — Безосновательно полагать, что все врачи будут иметь возможность просмотра EHR всех пациентов/лиц Канады посредством инфоструктуры EHR, так как в ней может содержаться несколько десятков тысяч субъектов данных. Как минимум VIP-персоны и другие элитные пациенты будут требовать ограничить доступ к их EHR, разрешив его только тем медицинским работникам, которые являются известными членами группы, предоставляющей им медицинскую помощь. Это функция по защите конфиденциальности, на которую канадцы обоснованно полагаются в вопросе защиты их ПМД от возможного случайного доступа лечащим врачом, зарегистрированным в инфоструктуре EHR. В данном случае, в свою очередь, требуется наличие определенного механизма для получения информации об отношении пациента/лица к его/ее

лечащему врачу. Такая информация может быть извлечена из EHR пациента/лица. Также может существовать необходимость в поддержании списка одной или нескольких рабочих групп, членом которой является пользователь. Примеры могут включать в себя хирургические бригады в определенной больнице или врачей с привилегиями доступа в определенной больнице. Такие рабочие группы позволяли бы установление отношения пользователя к пациенту/лицу на основе существующих отношений между субъектом и другими членами рабочей группы.

Важно отметить, что инфоструктура EHR не может считаться достоверным источником информации для всех присваиваний рабочих групп, так как эти присваивания являются очень нестабильными и изменяются слишком быстро, что не позволяет управлять ими централизованно. Предполагается, что системы POS при необходимости будут прослеживать такие присваивания (например, в информационной системе больницы) и что инфоструктура EHR будет полагаться на эти данные при наличии таковых. Предполагается, что инфоструктура EHR будет способна выводить заключения при условии, что между пациентом/лицом существуют надежные отношения, а такое отношение может быть логически получено из существующих ПМД (например, когда лечащий врач уже предоставил медицинские услуги пациенту/лицу, ввел данные в EHR пациента/лица, назначил обследование, выписал рецепт на лекарства).

Требование безопасности 63 канадской медицинской организации Infoway

Предоставление доступа пользователем на основе связи (ассоциации)

Инфоструктура EHR и все системы POS, подключенные к инфоструктуре EHR:

a) должны связывать пользователей (лечащих врачей) с картами пациента/лица и позволять дальнейший доступ на основе этой связи; т. е. они должны предоставлять дискреционный доступ к картам, основанный на том, что зарегистрированный пользователь, который уже имеет разрешение на доступ к карте пациента (картам пациентов), предоставил права доступа к этим картам другому зарегистрированному пользователю;

b) должны позволять пользователям предоставлять другим пользователям доступ к картам, если предоставляющие пользователи не располагают таким доступом к карте; обратите внимание на то, что предоставление доступа другим пользователям к карте не отменяет ограничения ролевой модели управления доступом для других пользователей.

Обоснование — Данное требование имеет существенное значение, если требование безопасности 60 должно точно соблюдаться. Как было отмечено ранее, дискреционное управление доступом не «превалирует» над ролевым управлением доступом. Например, врач общей практики может предоставить другому (специалисту) полный доступ к карте одного из своих пациентов. Специалист может позже воспользоваться доступом для выписки электронного рецепта для пациента. Однако если врач предоставляет доступ медсестре, медсестра не может позднее выписать электронный рецепт для пациента, так как ролевое управление доступом, как правило, будет предотвращать осуществление такой функции медсестрой.

Великобритания

Требование 3.3.2 Управления информацией Великобритании

Система должна использовать ролевую модель управления доступом для авторизации доступа пользователя к функциям и данным системы.

Требование 3.3.3 Управления информацией Великобритании (требование Великобритании, относящееся к конкретному случаю)

Система, которая объединяет ролевую модель управления доступом с CRS NHS, должна получать информацию о ролевом профиле, присвоенном пользователю, с помощью интерфейсов SAML, предусмотренных Spine для подобных целей, в соответствии с определением в Спецификации внешнего интерфейса Spine (EIS).

Требование 3.3.6 Управления информацией Великобритании

Система, которая объединяет ролевую модель управления доступом с CRS NHS, должна осуществлять установленное государством сопоставление для всего, от служебной роли/рабочей области до основной деятельности, в соответствии с публикацией уполномоченного органа.

Система должна периодически осуществлять процесс обновления сопоставлений, установленных государством для всего, от служебной роли/рабочей области до основной деятельности, в соответствии с публикацией уполномоченного органа время от времени.

Требование 3.3.7 Управления информацией Великобритании

В случае, если поставщику существующих систем не требуется поддерживать аутентификацию SSB, система должна использовать локальные средства управления доступом на основе ролей, которые поддерживают предоставление прав доступа в соответствии с установленными государством служебными ролями/рабочими областями и действиями. Такие локальные механизмы RBAC должны:

- ограничивать использование системы пользователями до выполнения конкретных функций, присваиваемых только менеджером(ами) системы;
- не позволять любым пользователям осуществлять доступ к выделенным для них функциям до тех пор, пока они не введут свою идентификационную информацию и пароль.

Средства контроля доступа должны включать возможность предоставления отдельного доступа к следующим функциям:

- просмотру аудиторского следа;
- доступу к информации о неработающем персонале;
- доступу к картам пациентов, который не может быть осуществлен обычным способом пользователями системы (например, в системах GP, к картам пациентов, которые на данный момент не используются в работе).

Требование 3.3.9 Управления информацией Великобритании

a) Система должна гарантировать, что организация выбранного профиля роли соответствует организации системы, вход в которую пытается осуществить пользователь, а также что она разрешает доступ, только если:

- организация а рамках выбранного профиля роли подбирает код организации в пределах системы или
- в условиях микрорайонных аптек роль и направление работы выбранного ролевого профиля совпадает с ролью и направлением работы пользователей-фармацевтов, а организация в рамках выбранного ролевого профиля соответствует специальной условной настройке организации (код организации FFFFF) для поддержки EPS R2. Система должна поддерживать использование ролевого профиля только FFFFF организации, если нет соответствующего специального ролевого профиля организации, связанного с пользователем.

b) На экране выбора ролевого профиля система должна отображать только те профили, которые применимы к системе, вход в которую пытается осуществить пользователь. Кроме того, любой ролевой профиль FFFFF организации будет отображаться только в том случае, если нет соответствующего специального ролевого профиля для этой организации. Система должна прояснить пользователю, какой ролевой профиль используется системой: как правило, наиболее подходящим будет только один ролевой профиль, в таком случае пользователю нет необходимости самому выбирать его из списка, который включает другие неподходящие (не соответствующие организации) или менее подходящие (для FFFFF организации) ролевые профили.

Требование 3.3.10 Управления информацией Великобритании

Поставщики должны предоставлять подробную информацию о сопоставлении своих локальных системных функций с действиями, выполняемыми в национальной базе данных RBAC, используя предоставленный образец. Это необходимо для поддержки процесса удаленного доступа (для того чтобы обеспечить наличие у Ras информации, необходимой для присвоения пользователям соответствующих служебных ролей, направлений работы и любых дополнительных действий), а также для поддержки процесса соответствия.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 5.11

Система должна предоставлять возможность установки ограничений или разрешений для пользователей/групп в соответствии с матрицей прав доступа.

B.7.2 Предоставление информации о правах доступа

Канада

Требование безопасности 63а канадской медицинской организации Infoway

Регистрация прав доступа пользователя

EHRi и все системы POS, подключенные к инфоструктуре EHR, должны предоставлять функции, которые позволяют обеспечить определенного пользователя следующей информацией:

a) к каким записям пользователь может осуществлять доступ;

b) к каким частям записи пользователь может осуществлять доступ;

c) какие права (просмотра, изменения и т. д.) имеет пользователь применительно к каждой из этих записей.

Обоснование — Прошлый опыт использования популярного программного обеспечения операционной системы показал, насколько сложным является определение того, имеет ли определенный пользователь доступ к определенной записи или может ли он использовать данную ему привилегию, если в системе не существует отдельной функции, отвечающей на такие вопросы. Отсутствие такой функции значительно усложняет обнаружение и устранение ошибок, возникающих при предоставлении пользователю прав доступа.

Великобритания

Требование 3.1.12 Управления информацией Великобритании

Данное приложение должно предоставить пользователям возможность проводить проверку роли и организации, имеющих значение для получения доступа, получаемого этими пользователями, так, чтобы они не могли заявить о незнании этой роли или организации или иными способами оправдать неосведомленность о значении своих действий.

B.7.3 Ограничение прав доступа

США

CCHIT SC 01.01

Контроль доступа

Система должна предоставлять наиболее ограниченный набор прав/привилегий или доступов, необходимых пользователям/группам (например, системным администраторам, секретарям, медсестрам, докторам) или процессам, действующим от имени пользователей, для выполнения указанных задач.

ИСО/МЭК 27002:2005, 9.1.1.2.b;

HIPAA: 164.312(a) (1); 164.308(a) (3) (1);

HITSP/TP20;

NIST SP 800-53: AC-6 ОРГАНИЧЕНИЕ ПРАВ;
AC-5 РАЗДЕЛЕНИЕ ОБЯЗАННОСТЕЙ.

Канада

Требование безопасности 59 канадской медицинской организации Infoway

Выбор отдельной роли для каждого сеанса

Все системы POS, подключенные к инфоструктуре EHR, должны гарантировать, что каждый пользователь будет осуществлять доступ к приложениям и службам инфоструктуры EHR на основании отдельной роли (т. е. пользователи, которые имеют несколько разных ролей, должны использовать отдельную роль для каждого сеанса инфоструктуры EHR).

Обоснование — Пользователи, имеющие несколько несопоставимых ролей, должны использовать их по отдельности. Например, врач общей практики, работающий в отделении неотложной помощи сельской больница один день в неделю (и имеющий право обхода ограничения в случае чрезвычайных обстоятельств при исполнении служебных обязанностей), должен четко указать в системе POS, что он действует в пределах данных ему полномочий, перед тем как осуществить доступ к EHR пациента/лица через инфоструктуру EHR. Другим примером является пользователь инфоструктуры EHR, осуществляющий доступ к EHR в качестве клинического врача, а также иногда в качестве исследователя.

Иерархическая структура ролей, включающая пользователей, которые часто выбирают между двумя ролями, каждая из которых относится к медицинской деятельности, позволит значительно снизить неудобство, вызванное необходимостью напрасной смены одной роли на другую.

См. также: ИСО/МЭК 27001:2005, А.11.2.2.

Великобритания

Требование 3.3.4 Управления информацией Великобритании

Система, которая объединяет CRS NHS с моделью RBAC, должна позволять пользователю выбирать, какой из присвоенных ему ролевых профилей он должен применять во время пользовательского сеанса с приложением. Если выбор не сделан, система должна применять тот ролевой профиль, который был выбран во время первого входа в CRS NHS.

Требование 3.3.5 Управления информацией Великобритании

Система, которая объединяет CRS NHS с моделью RBAC, должна позволять пользователю выбирать, какой из присвоенных ему ролевых профилей он должен применять во время пользовательского сеанса с приложением. Если выбор не сделан, система должна применять тот ролевой профиль, который был выбран во время первого входа в CRS NHS.

B.7.4 Передача прав на доступ

Бразилия

NGS1.04.07

Передача полномочий

Делегирующим является лицо, отвечающее за передачу полномочий, а делегатом является лицо, которому делегируются обязанности. Соответственно:

- делегирующий должен иметь предварительное разрешение на предоставление таких прав;
- передача полномочий должна регистрироваться в системе;
- при передаче должно быть указано следующее:
    - делегирующий;
    - делегат;
    - причина;
    - дата и время передачи;
    - период времени, на который предоставляется разрешение.

Примечание — Примером передачи полномочий является случай, при котором врач передает медсестре право на ввод информации о пациенте.

Канада

Требование безопасности 63 канадской медицинской организации Infoway

Предоставление доступа пользователем на основе связи

EHRi и все системы POS, подключенные к инфоструктуре EHR:

a) должны связывать пользователей (лечащих врачей) с картами пациента/лица и позволять дальнейший доступ на основе этой связи; т. е. они должны предоставлять избирательный доступ к картам, основанный на том, что зарегистрированный пользователь, который уже имеет разрешение на доступ к карте пациента (картам пациентов), предоставляет права доступа к этим картам другому зарегистрированному пользователю, и

b) не должны позволять пользователям предоставлять другим пользователям доступ к картам, если предоставляющие пользователи не располагают таким доступом по отношению к карте.

Необходимо обратить внимание на то, что предоставление доступа другим пользователям к медицинской карте не отменяет ограничения ролевой модели управления доступом для других пользователей.

Б.7.5 Отмена прав доступа

США

CCHIT SC 01.04

Контроль доступа

Система должна поддерживать возможность удаления привилегий пользователя, не удаляя пользователя из системы. Цель данного условия — предоставить возможность удаления привилегий, сохранив при этом историю действий пользователя в системе.

HIPAA: 164.308(a) (4) (ii) (C); 164.308(a) (3) (i) (C);

HITSP/TP20.

Канада

Требование безопасности 62 канадской медицинской организации Infoway

Своевременная отмена привилегий доступа

Инфоструктура EHR и все системы POS, подключенные к инфоструктуре EHR, должны поддерживать возможность своевременной отмены привилегий доступа пользователя, т. е. предотвращать вход пользователя в систему сразу же после отмены его привилегий доступа.

Обоснование — Данное требование гарантирует, что привилегии пользователя на доступ в инфоструктуру EHR могут незамедлительно и систематически приостанавливаться, если на это имеются причины.

В.8 Приемлемое использование

В.8.1 Уведомление пользователей

США

CCHIT SC 06.07

Технические службы

Система перед предоставлением доступа к любым ПМД должна отображать конфигурируемое уведомление или баннер при входе в систему (например, «Доступ к системе должен осуществляться только авторизованными пользователями»).

В случае если система не поддерживает возможность отображения баннера перед входом в систему, она должна отображать его сразу после авторизации.

CC2.1 L.4 Баннеры доступа TOE (FTA_TAB); CC3.0 FIA_TIN.1 Информационное предупреждающее сообщение;

NIST SP 800-53 AC-8 Уведомление об использовании системы;

HIPAA 164.308(a)(5)(i); 164.308(a)(5)(ii).

Великобритания

Требование 3.1.11 Управления информацией Великобритании

Приложение должно на видном месте отображать следующее сообщение при его запуске, чтобы напомнить пользователям об их обязательствах и правовых ограничениях на использование системы: Закон о неправомерном использовании компьютерных технологий 1990 г. «Несанкционированный доступ к этой системе является преступлением». Обратите внимание, что эта формулировка может периодически обновляться.

В.9 Безопасность сеанса

В.9.1 Время ожидания пользовательского сеанса

Бразилия

NGS1.03.01

Завершение сеанса при бездействии

Сеанс пользователя может быть завершен по истечении регулируемого периода бездействия путем отмены параметра управления сеансом, используя, например, файл cookie.

ABNTNBR ИСО/МЭК 27001:2005, A.11.5.5.

США

IFR.03

Завершение электронного сеанса по истечении предварительно установленного периода бездействия.

SC 03.03

Аутентификация

Система при обнаружении бездействия интерактивного сеанса должна предотвратить дальнейший просмотр и доступ к системе, используя этот сеанс, путем его завершения или блокировки, которая остается в силе до тех пор, пока пользователь не восстановит доступ с помощью соответствующих процедур идентификации и аутентификации. Время ожидания активности должно регулироваться.

Канада. Альберта 7.3.14 (безопасность);

Канада: Онтарио 5.6.12.a (защита рабочих станций);

ИСО/МЭК 15408, CC SFR: FTA_SSL, FMT_SAE;

NIST SP 800-53: AC-7 НЕУДАЧНЫЕ ПОПЫТКИ ДОСТУПА; AC-11 БЛОКИРОВКА СЕАНСА; AC-12 ЗАВЕРШЕНИЕ СЕАНСА;

HIPAA: 164.312(a) (1); 164.312(a) (2) (iii).

Канада

Требование безопасности 72 канадской медицинской организации Infoway

Ограничение доступа к автономным рабочим станциям

Все системы POS, подключенные к инфоструктуре EHR, должны защищать автоматически управляемые рабочие станции от посторонних лиц, пользующихся возможностью использования рабочей станции, пока система функционирует либо с помощью автоматического времени ожидания после бездействия, либо путем размещения рабочей станции на физически защищенном участке.

Обоснование — Многие клинические системы POS уже применили данное требование, по крайней мере на начальном уровне (например, автоматическое истечение срока ожидания после периода бездействия). Некоторые рабочие станции расположены на физически защищенных участках (например, за счетчиком дозировки лекарственных препаратов в аптеках). Надлежащее размещение рабочих станций также играет важную роль в обеспечении гарантии того, что пациенты/лица не смогут просматривать информацию, содержащуюся в картах других пациентов.

Великобритания

Требование 3.8.1 Управления информацией Великобритании

Система должна предоставлять средства контроля для защиты автоматически управляемых рабочих станций от посторонних лиц, включающие автоматическую блокировку по истечении периода бездействия; это может осуществляться путем применения программы предохранения экрана или блокировки приложения, требующих повторной аутентификации пользователя. Перед активацией автоматической блокировки появится предупреждение о том, что срок ожидания истекает (данное предупреждение будет отображаться в течение заданного периода времени перед блокировкой, период отображения по умолчанию составляет 60 с).

Требование 3.8.2 Управления информацией Великобритании

Система должна предоставлять пользователю средство, позволяющее заблокировать систему в одно действие, это действие скрывает любые идентифицируемые данные пациента от просмотра и обеспечивает необходимость повторной аутентификации для возобновления работы приложения.

Требование 3.8.3 Управления информацией Великобритании

Если пользователю отказано в доступе на основании требований, изложенных в этой статье, тот же пользователь может возобновить свой сеанс путем повторной аутентификации или любой другой пользователь может выйти из предыдущего сеанса (без его возобновления) для того, чтобы продолжить работу с помощью нового сеанса.

Требование 3.1.5 Управления информацией Великобритании

Система должна совмещать со службой Spine Security Broker механизмы сигнализации о:

- времени ожидания сеанса;
- времени ожидания активности;
- удалении смарт-карты;
- при получении уведомления об одном из этих событий система должна гарантировать, что пользователь пройдет повторную аутентификацию в соответствии с описанием, приведенным в требовании 3.1.4, перед тем как получить разрешение на дальнейшее использование системы CRS NHS;
- система должна осуществлять это путем регистрации службы Token Listener (слушатель событий маркеров) (см. спецификацию внешнего интерфейса и 3.1.6);
- следует обратить внимание на то, что значения сеанса и времени ожидания активности устанавливаются уполномоченным органом и периодически могут изменяться.

Требование 3.1.6 Управления информацией (для Великобритании)

SSO Token Listener (слушатель событий SSO-маркеров). Для определения окончания сеанса пользователя в соответствии с описанием в 3.1.5 система должна «слушать» события SSO-маркера.

Примечание — Сеанс пользователя Spine не зависит от сеанса пользователя аккредитованной службы.

Интерфейс SSOTokenListener посредника безопасности Spine (The Spine Security Broker, SSB) предоставляет механизм для приложений, которые требуют уведомления по истечении срока действия SSO — маркера. Срок действия маркера истекает по достижении максимального времени сеанса, максимального периода бездействия или при завершении сеанса администратором.

Система должна применять метод addSSOTokenListener, используя интерфейс SSOToken; данный метод реализует интерфейс SSOTokenListener. После истечения срока действия SSO-маркера будет использоваться объект обратного вызова. С помощью SSOTokenEvent (предоставленного посредством обратного вызова) система сможет определить время и причину истечения срока действия SSO-маркера.

При разрушении сеансового маркера SSB осуществляет зарегистрированный обратный вызов. Обратным вызовом является запрос HTTP POST, который передает данные XML специализированной серверной Java-программе в системе; система получает HTTP Post и использует информацию, содержащуюся в нем, для осуществления соответствующих действий.

Более подробная информация предоставлена в Спецификации внешнего интерфейса.

Требование 3.1.7 Управления информацией Великобритании
Система должна поддерживать активность пользовательского сеанса во время ее активного использования пользователем. Это достигается за счет использования соответствующих функций регенерации маркера с помощью API-интерфейса SSO, входящего в состав службы SSB.
Подобные функции регенерации, которые сбрасывают таймер бездействия в Spine, могут запускаться каждый раз, когда пользователь применяет функцию, которая взаимодействует с Spine (например, извлечение из PDS) или при использовании локального таймера бездействия, который вызывает восстановление перед тем, как активируется время ожидания активности Spine.

B.9.2 Время ожидания подключения

Канада

Требование безопасности 70 канадской медицинской организации Infoway
Ограничение времени установления соединения с приложениями инфоструктуры EHR
В соответствующих случаях инфоструктура EHR должна ограничивать длительность подключения к прикладным службам инфоструктуры EHR для обеспечения дополнительной безопасности доступа к таким приложениям.
Обоснование — Иногда данное требование применяется для приложений с высоким уровнем безопасности для обеспечения повторного подключения (и, следовательно, повторной аутентификации) в случаях, когда соединение оставалось отрытым в течение длительного периода времени. Длительность периода поддержки соединения меняется в зависимости от характера приложения и типов соединений (например, от сервера к серверу или от клиента к серверу). Учитывая структуру обмена сообщениями, определенную в макете EHRS, соединения с инфоструктурой EHR, как правило, длятся не более нескольких минут.

B.9.3 Безопасность сеанса

Бразилия

NGS1.03.02
Защита пользовательского сеанса от кражи
Сеанс связи должен быть обеспечен средствами контроля за безопасностью для предотвращения кражи пользовательского сеанса.

Примечание — Сеанс может быть «украден» даже во время защищенных сеансов (например, SSL/TLS). Например, если сеанс отслеживается посредством файла cookie в URL (унифицированный локатор ресурса), в некоторых ситуациях URL-сеанс пользователя может быть получен и использован другим пользователем путем присвоения личности предыдущего пользователя.

ABNTNBR ИСО/МЭК 27001:2005, A.10.8.

B.10 Поддержание доступности данных

B.10.1 Резервное копирование и восстановление

Бразилия

NGS1.05.01
Резервное копирование/восстановление
Система EHR должна предусматривать создание резервных копий, которые отвечают следующим требованиям:
- необходимо экспортировать атрибуты безопасности вместе с данными;
- следует убедиться в том, что при восстановлении из резервной копии все атрибуты защиты и их ассоциации были автоматически восстановлены без вмешательства администратора;
- следует убедиться в том, что производить экспорт и восстановление резервной копии может только пользователь с ролью оператора резерва, гарантировав, что пользователь не имеет прямого доступа к информации.

ABNT NBR ИСО/МЭК 27001:2005, A.10.5.
NGS1.05.02
Проверка целостности при восстановлении данных
Необходимо обеспечить средство контроля, которое гарантирует проверку целостности информации при создании и восстановлении резервной копии.
ABNT NBR ИСО/МЭК 27001:2005, A.10.5.

США

CCHIT SC 05.02
Технические службы
Система должна быть конфигурируемой для предотвращения порчи или потери уже введенных в систему данных в случае сбоя системы (например, интеграция с UPS и т. д.).
ИСО/МЭК 15408, CC SFR: FPT_RCV;
HIPAA 164.312(c) (1).
CCHIT SC 08.01
Резервное копирование/восстановление
Система должна иметь способность создания резервных копий прикладных данных, наборов удостоверений защиты, а также файлов журнала/результатов аудита.

Канада. Альберта 7.3.16 (безопасность);
ИСО/МЭК 15408, CC SFR: FDP_ROL, FPT_RCV;
HIPAA: 164.310(d)(1).
CCHIT SC 08.02
Резервное копирование/восстановление
Функциональные возможности восстановления системы должны приводить к возврату в полностью рабочее и безопасное состояние. Данное состояние должно включать в себя восстановление данных приложения, набора удостоверений защиты и файлов журнала/результатов аудита в их прежнее состояние.
Канада. Альберта 7.3.18.9 (безопасность);
ИСО/МЭК 15408, CC SFR: FAU_GEN;
NIST SP 800-53: AU-2 СОБЫТИЯ, ПОДВЕРГАЕМЫЕ АУДИТУ;
HIPAA: 164.310(d) (1).
CCHIT SC 08.03
Резервное копирование/восстановление
При необходимости круглосуточной ежедневной работы системы она должна запускать резервное копирование одновременно с работой приложения.
Канада. Альберта 7.4.2.5 (технический + D1I);
ИСО/МЭК 15408, CC SFR: FDP_ROL;
HIPAA: 164.310(d) (1).

Канада

Требование безопасности 30 канадской медицинской организации Infoway
Безопасное резервное копирование данных
Все организации, размещающие компоненты инфоструктуры EHR, должны:
a) осуществлять резервное копирование ПМД и данных, критически важных для безопасности (защиты), таким способом, который обеспечивает конфиденциальность, целостность и доступность данных;
b) хранить резервные копии данных в физически защищенной среде вне рабочего места.
Обоснование — Существуют различные технологии обеспечения конфиденциальности данных в процессе хранения. Такими технологиями могут быть кодирование или использование деидентифицированных данных.
Юрисдикции должны устанавливать необходимый уровень защиты, основываясь на аспектах риска, а также технических и функциональных аспектах.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)
Система должна осуществлять резервное копирование личных данных на переносные хранилища.
Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)
Должны существовать как минимум две копии программного обеспечения (ПО) подсистемы защиты.
Должны существовать инструменты для восстановления как минимум двух копий ПО подсистемы защиты.
Целостность ПО подсистемы защиты должна проверяться при каждом повторном запуске операционной системы.

B.11 Защита данных в процессе передачи

B.11.1 Кодирование данных в процессе передачи

Бразилия

NGS1.06.01
Безопасность связи между клиентом и сервером.
Сеанс связи между компонентом клиента (сторона пользователя) и компонентом сервера должен вовлекать следующие службы защиты: аутентификации сервера, целостности данных и конфиденциальности данных.

Примечание — Примерами являются такие протоколы, как HTTPS (HTTP + SSL/TLS) и IPSEC.

ABNT NBR ИСО/МЭК 27001:2005, A.10.9.2 и A 10.6.
NGS1.06.03
Ограничение на передаваемые данные
При удаленном доступе к EHR компоненту клиента (сторона пользователя) должны передаваться только те данные, которые представлены пользователю. Это означает, что любая возможная обработка данных, связанная с выбором данных, должна осуществляться стороной сервера.
ABNT NBR ИСО/МЭК 27001:2005, A.10.9.2.
NGS1.06.04
Безопасность связи между компонентами
Если EHR состоит из нескольких распределенных компонентов (т. е., расположенных на разных компьютерах), то связь между этими компонентами (например, база данных) должна быть обеспечена следующими

компонентами безопасности: аутентификацией партнера (клиент или сервер), целостностью данных и конфиденциальностью данных.

ABNT NBR ИСО/МЭК 27001:2005, А.10.9.2.

США

CCHIT SC 06.01

Технические службы

Система должна поддерживать защиту конфиденциальности всей закрытой медицинской информации (ЗМИ), передаваемой по сети Интернет или другим открытым сетям, с использованием шифрования посредством тройного стандарта шифрования DES (3DES) или продвинутого стандарта шифрования (AES), а также таких открытых протоколов, как TLS, SSL, IPSec, шифрование XML или S/MIME или их преемников.

Канада. Альберта 7.4.6.2 и 8.4.6.2 (технический);

ИСО/МЭК 15408, *CC SFR: FCS_COP; FIPS 140-2;*

NIST SP 800-53: SC-13 КРИПТОГРАФИЧЕСКИЕ ОПЕРАЦИИ;

HIPAA: 164.312(e) (1); 164.312(a) (2) (iv);

HITSP T17;

FIPS PUB 140-2.

CCHIT SC 06.03

Технические службы

Системы, которые предоставляют доступ к ПМД через интерфейс веб-браузера (т. е. HTML через HTTP), должны включать в себя возможность шифрования данных, передаваемых по сети через SSL (HTML по HTTPS).

Примечание — Интерфейсы веб-браузера часто используются за пределами защищенной сети предприятия

ИСО/МЭК 15408, *CC SFR: AGD_ADM; HITSP/TP17;*

HIPAA: 164.312(e)(1); 164.312(a)(2)(iv).

CCHIT IFR.07

Необходимо убедиться в том, что электронная медицинская информация не была изменена в процессе передачи, и выявить изменения и удаление электронной медицинской информации и журналов аудита в соответствии со стандартом, указанным в таблице 2В, строка 4.

Таблица 2В, строка 4. Проверка того, что электронная медицинская информация не была изменена в процессе передачи: для проверки того, что электронная медицинская информация не была изменена в процессе передачи, должен использоваться безопасный алгоритм хеширования. В качестве безопасного алгоритма хеширования необходимо использовать SHA-1 или алгоритм более высокого уровня [например, публикация (PUB) Федерального стандарта по обработке информации (FIPS) Стандарт по безопасному хэшированию (SHS) FIPS PUB 180-3].

CCHIT SC 06.04

Технические службы

Система должна поддерживать защиту целостности всей закрытой медицинской информации (ЗМИ), передаваемой по сети Интернет или другим открытым сетям, через хеширование SHA-1 или SHA-256 или их преемников, а также через такие открытые протоколы, как TLS, SSL, IPSec, цифровая подпись XML или S/MIME или их преемники.

ИСО/МЭК 15408, CC SFR: FPT_RCV; FIPS 140-2; SP800-53: SC-13 КРИПТОГРАФИЧЕСКИЕ ОПЕРАЦИИ;

HIPAA: 164.312(e) (1); HITSP T17.

Канада

Требование безопасности 31 канадской медицинской организации Infoway

Кодирование ПМД в процессе передачи

В ходе передачи ПМД EHRi и системы POS, подключенные к инфоструктуре EHR, должны применять алгоритмы и протоколы шифрования информации, соответствующие промышленным стандартам. Это делается для поддержки конфиденциальности и целостности данных в тех случаях, когда передача данных происходит за пределами границ физической защиты, обеспечивающей безопасность средств обработки информации, поддерживающих серверы, приложения или данные EHR.

Обоснование — Перехват конфиденциальной информации представляет серьезный риск, а ее изменение в процессе передачи приводит к серьезным последствиям. Обеспечение конфиденциальности и целостности ПМД, передаваемых инфоструктурой EHR является минимальным требованием.

Медико-информационное законодательство не содержит конкретных инструкций относительно защиты информации в процессе передачи, однако существуют некоторые общие требования. Например, согласно медико-информационному законодательству провинции Онтарио хранителям информации требуется «передавать» ПМД безопасным способом. Согласно медико-информационному законодательству провинции Манитоба доверенному лицу, использующему электронные средства для осуществления запроса на раз-

глашение данных и получения ответа на такие запросы, требуется осуществлять меры по предотвращению перехвата информации посторонними лицами.

Требование безопасности 32 канадской медицинской организации Infoway

Защита целостности источника и адресата во время передачи ПМД

Инфоструктура EHR должна защищать источник и адресат сообщения от нелегального проникновения во время передачи ПМД для поддержки их конфиденциальности и целостности.

Обоснование — Данное требование является минимальным для защиты от угрозы нелегального проникновения. Это требование улучшает надежный двухточечный информационный поток и предусматривает реализацию таких технологий, как цифровые подписи, выделенные линии или виртуальные частные сети для защиты источника и адресата.

Великобритания

Требование 3.10.3 Управления информацией Великобритании

Для защиты конфиденциальности и целостности информации в процессе передачи система должна применять криптографические методы, которые соответствуют криптографическим стандартам NHS (периодически выпускаемые уполномоченным органом и предоставляемые по запросу, направленному на электронную почту esp.ig@nhs.net). Использование незашифрованных протоколов в качестве удаленного инструмента поддержки будет ограничиваться технической поддержкой или поддержкой программного обеспечения системы и не будет использоваться для получения доступа к персональным или конфиденциальным персональным данным.

Требование 3.11.18 Управления информацией Великобритании

В случаях когда услуга, предложенная поставщиком, требует передачи идентифицируемых данных пациентов с помощью электронных средств, то шифрование этих данных должно соответствовать уровню, который требуется утвержденными криптографическими стандартами. Эти зашифрованные данные могут передаваться через службу защищенной электронной почты, например почта NHS, или через утвержденную сеть, например N3.

Требование 3.10.2 Управления информацией Великобритании

Система должна обеспечивать конфиденциальность и целостность персональных данных и конфиденциальных персональных данных пациента в процессе передачи через ненадежные сети, включая (в числе прочего) передачу между:

- центрами обработки данных;
- центрами обработки данных и местом развертывания сетей LAN;
- клиентами N3 и устройствами удаленного доступа и
- центрами обработки данных и устройствами удаленного доступа.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.1

Система должна обеспечивать защиту всех личных данных, полученных через сеть Интернет или другие известные открытые сети, используя криптографические методы. Любой трансграничный обмен персональными данными должен быть защищен с помощью криптографических методов.

В.11.2 Подтверждение получения данных

Бразилия

NGS1.07.08

Подтверждение получения

Обмен данными между EHR должен быть обеспечен средствами контроля для подтверждения доставки/получения данных.

Примечание — Соответствующий пример находится в TISS.

ABNT NBR ИСО/МЭК 27001:2005, A 10.6.

Канада

Требование безопасности 33 канадской медицинской организации Infoway

Подтверждение получения переданных ПМД

В соответствующих случаях инфоструктура EHR должна получать подтверждение приема данных в процессе передачи ПМД для обеспечения гарантии того, что переданные данные были получены.

Обоснование — Подтверждение приема сообщения путем квитирование установления связи или другим методом является минимальным требованием для обеспечения полного получения информации адресатом.

В.12 Защита данных в процессе хранения

В.12.1 Защита данных в хранилищах данных

Бразилия

NGS1.04.01

Предотвращение несанкционированного доступа, осуществляемого посторонними лицами

Запретите неаутентифицированным посторонним сторонам доступ к EHR-S и DBMS.

HL7 ERH-S FM IN1.2 ABNT NBR ИСО/МЭК 27001:2005, A.11.6.1.

NGS1.04.02

Механизм управления доступом к EHR

Необходимо убедиться в том, что доступ к EHR возможен только через механизм управления доступом.

HL7 ERH-S FM IN1.2.

NGS1.07.05

Использование SGBD

Система управления базами данных (SGBD) должна хранить и обеспечивать защиту EHR

NGS1.07.06

Предотвращение прямого доступа к SGDB

Пользователи EHR не должны иметь прямой доступ к SGBD. Доступ пользователя к EHR должен позволяться только при использовании компонента управления доступом к EHR и аутентификации, прямой доступ к SGBD должен быть запрещен за исключением случаев, когда выполняется резервное копирование.

NGS1.07.07

Зашифрованные идентификационные данные пациента

Любые данные, идентифицирующие пациента, должны быть зашифрованы для предотвращения восстановления их EHR путем несанкционированного доступа к базе данных EHR или резервной копии (созданной для защиты данных).

ABNT NBR ИСО/МЭК 27001:2005A 10.7.3.

США

CCHIT IFR.05

Необходимо выполнить шифрование и дешифрование электронных медицинских данных в соответствии с параметрами, определенными пользователем (например, при резервном копировании, на съемных носителях информации, при входе/выходе из системы), согласно стандартам, указанными в таблице 2B, строка 1.

Таблица 2B, строка 1. Общее шифрование и дешифрование электронных медицинских данных: Должен использоваться симметричный криптографический алгоритм для фиксированного блока на 128 бит, способный использовать ключ шифрования 128, 192 или 256 бит [например, FIPS 197 Advanced Encryption Standard, (AES), Nov 2001].

Канада

Требование безопасности 36 канадской медицинской организации Infoway

Защита хранилищ данных

Все организации, размещающие компоненты инфоструктуры EHR, должны обеспечить защиту электронных носителей, содержащих ПМД или данные системы с особыми требованиями по информационной безопасности, включая регистрационные данные пользователей, с помощью одного или нескольких средств:

a) физической защиты носителей в соответствии с требованием безопасности 18;

b) надежной деидентификации персональных медицинских данных, хранящихся на них, или

c) шифрования данных, хранящихся на них.

Обоснование — Защита ПМД имеет важное значение, если использование и разглашение данной информации должно контролироваться. В этом смысле данное требование вытекает из требования безопасности 4.5. Шифрование хранилищ данных по-прежнему встречается редко в здравоохранении, и медицинские организации не спешат использовать современные технологии для шифрования баз данных. Попытки деидентифицировать данные, хранящиеся в базах данных, как правило, недостаточны и часто легко устраняемы.

Защита регистрационных данных пользователя играет важную роль для поддержания их полноты (и, соответственно, целостности процесса аутентификации пользователя). Защита их конфиденциальности также имеет существенное значение для поддержания доверия поставщиков медицинских услуг (которые, к примеру, не хотят получать маркетинговые материалы от спамеров, получивших доступ к слабозащищенным контактным данным). Несмотря на то что физическая защита хранилищ данных всегда будет иметь существенное значение (для защиты работоспособности системы), в соответствующих случаях при проектировании новых систем следует рассматривать деидентификацию и шифрование.

Великобритания

Требование 3.11.2 Управления информацией Великобритании

Система должна гарантировать, что данные CRS NHS, включая персональные и конфиденциальные персональные данные пациента, а также журналы аудита, защищены от несанкционированного доступа и внесения изменений в процессе хранения этих данных в базах данных и/или файлах.

B.12.2 Защита данных на портативных носителях

См. также ИСО/МЭК 27001:2005, A.10.8.3.

США

CCHIT SC 06.06

Технические службы

При хранении ПМД на любых портативных/съемных устройствах (например, флеш-накопитель, CD-ROM, PDA или портативный компьютер) система должна поддерживать использование основанного на стандартах

формата шифрования, применяющего стандарт тройного шифрования данных (3DES), продвинутый стандарт шифрования (AES) и преемников этих стандартов.
FIPS 140-2, ИСО/МЭК 15408, CC SFR: FCS_COP, OMB M-06-16, SP800-53: AC-19, HITSP T33; HIPAA: 164.312(e) (2) (ii); FIPS PUB 140-2.

Канада

Требование безопасности 34 канадской медицинской организации Infoway
Защита ПМД на портативных носителях
Все организации, размещающие компоненты инфоструктуры EHR, и организации, подключенные к инфоструктуре EHR, должны гарантировать, что ПМД и другие данные системы с особыми требованиями по информационной безопасности, хранящиеся на портативных носителях:
a) зашифрованы при передаче носителя для защиты целостности и конфиденциальности данных и
b) защищены от кражи в соответствующих случаях при передаче носителя для защиты доступности данных.
Обоснование — Данное требование предназначено для обеспечения защиты информации, хранящейся на съемных носителях. Мобильные устройства рассмотрены в требовании безопасности 73 (приемлемое использование мобильных устройств).

Великобритания

Требование 3.11.8 Управления информацией Великобритании
В случаях, когда устройства или услуги, предложенные поставщиком, требуют передачи любых идентифицируемых данных пациентов на любых портативных носителях, необходимо выполнить шифрование этих данных. Уровень шифрования должен соответствовать утвержденным криптографическим стандартам, описанным в требовании 3.10.3.
Требование 3.11.9 Управления информацией Великобритании
Шифрование, дешифрование, передача, хранение и уничтожение переносимых данных должны подвергаться аудиту, а носители должны регистрироваться в журнале и отслеживаться для обеспечения того, что все экземпляры включены в отчет.
Требование 3.11.11 Управления информацией Великобритании
Поставщик должен гарантировать, что применяемый продукт шифрования соответствует FIPS 140-2 и проходил аккредитацию CCTM (см. http://www.cesg.gov.uk/servicecatalogue/CCTM/Pages/ CCTM.aspx).
Требование 3.11.12 Управления информацией Великобритании
Поставщик должен гарантировать, что стойкость и сложность ключа шифрования для каждого архива соответствует описанию в утвержденном криптографическом стандарте.
Требование 3.11.13 Управления информацией Великобритании
В случаях когда ключи шифрования создаются системой автоматически для передачи данных на портативных носителях, система должна передать ключ шифрования на блок управления данными для каждой процедуры шифрования. В таких случаях криптографические ключи не должны быть созданы путем использования алгоритма или другого совместно используемого секретного ключа, который объединяет только известную или доступную информацию, касающуюся окружающей среды, или другую информацию, зависящую от контекста, без включения уникальной, зависящей от контекста секретной информации, в соответствии с требованиями пользователя или поставщика. Секретная информация, зависящая от контекста, должна контролироваться и управляться в соответствии с принципами рекомендуемых норм управления ключами защиты.
Требование 3.11.14 Управления информацией Великобритании
Поставщик должен гарантировать, что любые ключи шифрования, создаваемые системой, хранятся надежным способом для обеспечения возможности восстановления данных в случае утраты ключа или его порчи блоком управления данными.
Требование 3.11.15 Управления информацией Великобритании
Поставщик должен гарантировать, что ключ шифрования является уникальным для каждого архива данных.
Требование 3.11.16 Управления информацией Великобритании
В случаях когда система поставщика предоставляет механизм для отправки ключа шифрования получателю электронным путем или вручную, необходимо наличие на месте процессов для обеспечения гарантии того, что ключи шифрования отправлены вслед за отдельным механизмом связи для зашифрованных данных или отправлены отдельно от зашифрованных носителей.
Требование 3.11.17 Управления информацией Великобритании
В случаях когда услуга, предложенная поставщиком, требует передачи идентифицируемых данных пациентов на любых портативных носителях, необходимо выполнить шифрование этих данных, уровень которого должен соответствовать утвержденным криптографическим стандартам, и передать их безопасным способом. Передача идентифицируемых данных пациента должна проводиться с помощью безопасных служб доставки в соответствии с руководством по шифрованию Департамента здравоохранения.
См. также требование 3.11.7 Управления информацией Великобритании.

Российская Федерация
Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.1
Система должна обеспечить защиту всех медицинских данных, полученных по сети Интернет или по другим известным открытым сетям, с помощью криптографических методов. Любые подключения к сети Интернет или другим известным открытым сетям должны быть защищены с помощью системы сетевой защиты.
Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательная)
Любые портативные/съемные устройства, используемые для хранения персональных данных, должны быть маркированы и зарегистрированы в журналах аудита.

В.13 Целостность данных

В.13.1 Проверка целостности данных
Бразилия
NGS1.07.04
Проверка целостности данных
Необходимо наличие средств контроля для проверки целостности данных EHR для предотвращения действий пользователя или системных сбоев, которые приводят к противоречивости данных.
В.13.2 Импорт данных
Бразилия
NGS1.07.01
Импорт данных
Данные, импортированные из других EHR с помощью портативного устройства, должны быть соотнесены с пациентом и лечащим врачом, местом, датой и временем импорта, а также пользователем, который осуществил импорт данных.
HL7 ERH-S FM IN1.6.
В.13.3 Целостность данных в процессе импорта
Бразилия
NGS1.07.02
Ограничение передачи и экспорта EHR
EHR должны передаваться и экспортироваться только в следующих случаях:
- для переноса в другую систему;
- для резервного копирования;
- для передачи пациенту по его запросу в электронном или печатном формате;
- при процессах, требующих печати всей EHR или ее части;
- для обеспечения соответствия законодательными требованиям, для которых необходимы печатные документы.

Все действия по передаче и экспорту EHR должны быть записаны.
США
SC 06.13
Технические службы
Разглашение данных, содержащихся в картах, выполненное для лечения, оплаты и выполнения медицинских процедур, соответствует стандарту, указанному в таблице 2В, строка 6.
Таблица 2В, строка 6. Разглашение данных для лечения, оплаты и медицинских процедур: дата, время, идентификационные данные пациента (имя или номер), идентификационные данные пользователя (имя или номер) и описание причины разглашения должны быть зарегистрированы.
В.13.4 Проверка исходящих данных
Канада
Требование безопасности 78 канадской медицинской организации Infoway
Проверка печатных данных
Все системы POS должны обеспечивать возможность проверки полноты печатных копий документа (например, «страница 3 из 5»).
Обоснование — Эти требования являются минимальными для обеспечения целостности данных. Они предотвращают секретное, выборочное отображение данных.
См. также ИСО/МЭК 27001:2005, А.12.2.4.
Великобритания
Требование 3.17.5 Управления информацией Великобритании
Поставщик должен гарантировать, что система предоставляет средства, обеспечивающие пользователя возможностью проверки полноты печатных копий документа (например, маркировка «страница 3 из 5»).

В.14 Хранение данных

Канада
Требование конфиденциальности 21 канадской медицинской организации Infoway
Хранение данных
Инфоструктура EHR, системы POS, подключенные к инфоструктуре EHR, организации, подключающиеся к инфоструктуре EHR, и организации, размещающие компоненты инфоструктуры EHR, должны:

a) осуществлять хранение ПМД в соответствии с требованиями хранения документации, отраженными в законодательных актах, и
b) разрабатывать руководства и осуществлять процедуры, касающиеся хранения ПМД, включая минимальные и максимальные периоды хранения.
Обоснование — Это представляется достаточно сложным для устаревших систем и систем, основанных на хранении на бумажных носителях; среда электронного учета здоровья должна быть разработана для систематической реализации таких правил. В то же время пациенты/лица должны признать необходимость постоянного хранения основной информации о них в системе здравоохранения.

Великобритания

Требование 3.11.6 Управления информацией Великобритании
Система должна гарантировать, что все данные хранятся в течение периодов, установленных политикой DH и описанных в Практическом руководстве NHS по управлению документооборотом, части 1 и 2.

B.15 Маркировка данных

Канада

Требование безопасности 11 канадской медицинской организации Infoway
Нанесение маркировки о конфиденциальности персональных медицинских данных
Все системы POS, подключенные к инфоструктуре EHR, должны информировать каждого пользователя POS о конфиденциальном характере ПМД:
a) путем отображения маркировки на печатной копии, отображающей данные, или
b) путем отображения данной маркировки на любом экране, отображающем данные, или
c) путем отображения данной маркировки пользователю сразу после входа в приложение POS (возможно, в рамках политики допустимого использования).
Обоснование — Данное требование гарантирует, что все поставщики медицинских услуг и обслуживающий персонал осведомлены о том, что конкретная информация, просматриваемая ими, является конфиденциальной. Это особенно важно в случае, если информация содержится в электронных письмах, факсах и других документах, которые могут содержать конфиденциальную и не конфиденциальную информацию одновременно. Известно, что заявления о приемлемом использовании могут быть не замечены после нескольких использований системы. Основным преимуществом постоянного отображения таких заявлений является обеспечение основания для привлечения к уголовной ответственности пользователей, которые не отнеслись к информации с должным вниманием (т. е. не обращались с информацией как с конфиденциальной).

Великобритания

Требование 3.17.1 Управления информацией Великобритании
Поставщик должен гарантировать, что все личные данные пациента, которые выводятся из медицинского приложения, предоставляемые в рамках данного соглашения, маркируются надписью «Конфиденциально NHS: личные данные пациента». Кроме того, поставщик должен соблюдать такие требования к маркировке, которые могут быть обоснованно указаны уполномоченным органом, например, для отображения изменений в соответствующем законодательстве. Обратите внимание на то, что требования в данном разделе не должны влиять на спецификации печати для рецептов или раздачи маркеров в соответствии с требованиями EPS. Дальнейшее руководство представлено по адресу:
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/nhsinforiskmgt.
Требование 3.17.2 Управления информацией Великобритании
Служба должна предусматривать защитную маркировку информации, которую необходимо довести до сведения каждого пользователя в соответствии с 3.17:
a) путем представления на любом экране, отображающем информацию, или
b) путем отображения пользователю сразу после входа в систему (возможно, в рамках политики допустимого использования).
Требование 3.17.3 Управления информацией Великобритании
При выборе варианта a) в требовании 3.17.2 исполнитель должен гарантировать, что защитная маркировка информации отображена стандартизированным образом и в соответствующем стандарту месте на любом экране, отображающем информацию.
Требование 3.17.4 Управления информацией Великобритании
Поставщик должен гарантировать, что защитная маркировка информации отображена стандартизированным образом и в соответствующем стандарту месте на любой печатной копии, отображающей информацию.

B.16 Проведение аудита

B.16.1 Журналы аудита и события триггера

Бразилия

NGS1.08.04
Журналы аудита
Журналы аудита должны содержать информацию, как минимум связанную со следующими событиями:
- попытками аутентификации пользователя;

- действиями по управлению пользователем, ролью и группой;
- действиями по управлению системой;
- действиями, выполняемыми пользователями;
- взаимодействием с другими системами, включая другие EHR;
- обменом данными (передача и получение);
- резервным копированием;
- осуществлением доступа к базе данных.

По отношению к вышеперечисленным событиям журналы аудита должны содержать как минимум следующую дополнительную информацию о каждом событии:

- дату и время;
- место;
- пользователя.

ABNT NBR ИСО/МЭК 27001:2005, A.10.10.1; ИСО 18308:2011(E) PRS5.3.

США

CCHIT SC 02.03

Аудит

Система должна иметь возможность обнаружения событий, связанных с безопасностью, которые она опосредует и для которых создает журналы аудита. События как минимум включают перечисленные в приложении «События, прошедшие аудит»:

Примечание — Система отвечает только за аудит тех событий безопасности, посредником которых она является. Опосредованным событием является событие, в котором система принимала активное участие, или приводила к его возникновению, или имела возможность его обнаружения. Система не создает записи в журнале аудита для тех событий безопасности, к которым она не причастна.

a) запуск/остановка;
b) вход/выход пользователя из системы;
c) время ожидания сеанса;
d) блокировка учетной записи;
e) создание/просмотр/обновление/удаление карты пациента;
f) планирование;
g) запрос;
h) заказ;
i) сбой аутентификации узла;
j) создание/проверка подлинности подписи;
k) экспорт ПМД (например, распечатка);
l) импорт ПМД;
m) события управления системой защиты;
n) резервное копирование и восстановление.

ИСО/МЭК 15408, *CC SFR: FAU_GEN;*

NIST SP 800-53: AU-2 СОБЫТИЯ, ПОДВЕРГАЕМЫЕ АУДИТУ;

HIPAA: 164.312(b); 164.312(1); 164.308 (a)(1)(ii)(A) and (D); HITSP/TP15.

CCHIT IFR.10

Разглашение данных, содержащихся в картах, выполненное для лечения, оплаты и медицинских процедур, соответствует стандарту, указанному в таблице 2B, строка 6.

Таблица 2B, строка 6. Разглашение данных для лечения, оплаты и медицинских процедур: дата, время, идентификационные данные пациента (имя или номер), идентификационные данные пользователя (имя или номер) и описание причины разглашения должны быть зарегистрированы.

Канада

Требование конфиденциальности 19 канадской медицинской организации Infoway

Регистрация доступа, изменения и разглашения

Все системы POS, подключенные к инфоструктуре EHR, должны:

a) иметь механизм для регистрации каждой попытки доступа, изменения или разглашения ПМД с указанием времени и идентификационных данных пользователя, осуществляющего доступ;

b) иметь механизм для регистрации каждой попытки доступа, изменения или разглашения регистрационных данных провайдера или пользователя (включая данные идентифицируемых лечащий врачей и других пользователей инфоструктуры EHRi, например, их имена, адреса, информацию о лицензии на деятельность и другую регистрационную информацию пользователя; регистрационные данные провайдера не относятся к медицинским) с указанием времени и идентификационных данных пользователя, осуществляющего доступ;

c) в случаях, определенных законом, иметь механизмы для предупреждения членов организации, ответственных за обеспечение конфиденциальности (см. требование конфиденциальности 1), когда существует подозрение, что ПМД обрабатывались, использовались или разглашались несоответствующим образом.

Обоснование — В соответствии с требованиями специального законодательства организациям необходимо регистрировать попытки доступа, изменения и разглашения ПМД. В случаях когда доступ, использование и разглашение не соответствуют тому, что разрешено инфоструктурой EHR, лица, ответственные за соблюдение конфиденциальности, должны быть уведомлены.

Журналы регистрации доступа, изменения и разглашения сами по себе содержат конфиденциальную информацию и, следовательно, должны иметь защиту и исключать несанкционированный доступ. Требования к их безопасности описаны в требованиях безопасности 38—52. Для получения информации по регистрации директив согласия см. требование конфиденциальности 13.

Требование безопасности 42 канадской медицинской организации Infoway

Регистрация доступа к ПМД в системах POS

Все системы POS, подключенные к инфоструктуре EHR, должны заносить в журнал аудита каждый случай осуществления пользователем доступа, обновления или архивации ПМД.

Обоснование — Данное требование вытекает из требования безопасности 19.

Требование конфиденциальности 22a канадской медицинской организации Infoway

Обозначение пациентов/лиц с повышенным риском

Инфоструктура EHR должна предоставить функции для маркировки записей выбранных пациентов/лиц и впоследствии подвергать доступы к таким субъектам данных обязательному аудиту, проводимому лицом, ответственным за соблюдение конфиденциальности в организации.

Обоснование — Это требование значительно облегчает выявление подозрительных или неправомерных случаев использования привилегий доступа, касающихся пациентов, которые являются знаменитыми или чья конфиденциальность иным образом находится под существенной угрозой.

Карты определенных пациентов/лиц (например, политики, знаменитые и известные личности) могут находиться под существенной угрозой получения доступа к ним лицами, которые не имеют служебной необходимости. Поэтому, возможно, целесообразным является разместить на этих картах дополнительные средства управления аудитом для того, чтобы защитить конфиденциальность пациента. Инфоструктура должна признать практичность такого метода и способствовать быстрому и регулярному проведению аудита доступа к этим записям (возможно, включая уведомление сотрудника по обеспечению конфиденциальности о каждом доступе). Данное требование не должно рассматриваться как означающее, что информация в картах такого пациента/лица некоторым образом является более конфиденциальной, чем информация обычных граждан, или что эти карты как информационный ресурс являются более ценными, чем те, для которых не повышен риск неприемлемого доступа. Наоборот, требование гарантирует наличие возможностей для быстрого выявления чрезмерного интереса со стороны пользователей, которые не имеют законной необходимости ознакомления с конфиденциальной информацией.

Для ознакомления с требованиями по ведению журнала аудита, связанными с данным требованием конфиденциальности, см. требование безопасности 49.

Требование безопасности 38 канадской медицинской организации Infoway

Регистрация операций в инфоструктуре EHR

Инфоструктура EHR должна создавать защищенные протоколы с результатами аудита каждый раз, когда пользователь:

a) осуществляет доступ, создает или обновляет ПМД пациент/лица через инфоструктуру EHR;

b) игнорирует директивы согласия пациента/лица через инфоструктуру EHR;

c) через инфоструктуру EHR осуществляет доступ к данным, которые были защищены или скрыты в соответствии с указанием пациента/лица, или

d) осуществляет доступ, создает или обновляет регистрационные данные пользователя инфоструктуры EHR.

Обоснование — Протоколы с результатами аудита должны содержать необходимую информацию, позволяющую дать ответ на следующие вопросы:

- в случае заданного пользователя, к каким ПМД был осуществлен доступ, какие ПМД были созданы или обновлены и когда;

- в случае определенного элемента ПМД, какие пользователи получили к ним доступ, создали их или обновили и когда.

Данное требование вытекает из требования конфиденциальности 13 и требования конфиденциальности 19, и его выполнение также необходимо для эффективного соблюдения законодательства в некоторых юрисдикциях. Оно также вытекает из требования конфиденциальности 6, требования конфиденциальности 13 и требования конфиденциальности 24.

Информация об аудите может храниться в системах POS, а также в инфоструктуре EHR. Для того чтобы подготовить официальный письменный протокол, содержащий информацию о том, какие пользователи осуществляли доступ к ПМД пациента/лица или к каким ПМД пользователь осуществлял доступ, все записи

о результатах аудита должны быть открыты для доступа, что делает соответствие требований по аудиту самым строгим существующим юрисдикционным законодательным требованиям незаменимым для обеспечения полной совместимости (интероперабельности) с разными юрисдикциями.

Совместимость также лежит в основе последовательного и единого ведения журналов (регистрации). Несмотря на то что в Канаде не существует широко применяемого стандарта для ведения медицинских журналов аудита, стандарт IHE «Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications» описывает XML-схему для предоставления информации, необходимой для аудита конфиденциальности и безопасности медицинских приложений. Данный стандарт выпускается под общей редакцией с IHE IT Infrastructure Technical Framework Supplement 2004—2005, Audit Trail and Node Authentication Profile Public Comment Version.

Требование безопасности 41 канадской медицинской организации Infoway

Регистрация (ведение журнала) передачи ПМД в инфоструктуре EHR

Инфоструктура EHR должна определять всех прошлых получателей данных от EHR, а также уведомлять их в случае, если в дальнейшем данные в EHR были изменены.

Обоснование — Данное требование облегчает проведение общесистемного аудита передачи и получения сообщений. Оно также вытекает из требования безопасности 25.

Несмотря на то что регистрация всех последних получателей в журналах может значительно увеличиться в числе, стоимость оперативного хранения продолжает сокращаться в два раза каждый год, и даже терабайт памяти больше не представляется чрезмерно дорогим для многих медицинских организаций.

Инфоструктура EHR может требовать сохранения всех записей обо всех случаях обмена ПМД между юрисдикциями. Данное требование основано на юрисдикционном законодательстве. Например, законодательные акты по медицинской информации провинции Альберта, согласно которым хранителю, разглашающему ПМД, необходимо записывать имя человека, которому хранитель разглашает информацию, дату и цель разглашения, а также описание разглашенной информации. Последнее требование (описание разглашенной информации) не соответствует предыдущему требованию полностью, однако в этом случае предыдущее требование необходимо соблюдать наряду с другими требованиями к ведению журнала аудита, указанными в данном разделе.

Великобритания

Требование 3.15.4 Управления информацией Великобритании

Успешный вход в систему, неудачные попытки входа в систему и выход из системы, а также изменения пароля должны регистрироваться в системном журнале аудита. Данные, которые необходимо включить в запись в журнале аудита:

- успешный вход в систему, выход из системы:
    - идентификатор пользователя;
    - дата и время;
- неудачная попытка входа в систему:
    - количество попыток;
    - дата и время;
    - точка доступа (при наличии);
    - идентификатор пользователя (при наличии);
- изменения паролей:
    - идентификатор пользователя;
    - пользователь, пароль которого изменен;
    - дата и время;
- подобные записи в журнале аудита также должны включать в себя идентификационную информацию оконечного устройства (или системы).

Требование 3.9.11 Управления информацией Великобритании

Журналы аудита должны включать в себя подробную информацию о каждой конфигурации (например, о включении службы spine service) или изменениях справочной информации (например, об обновлении данных клинической схемы кодирования, базы данных лекарственных препаратов), применяемых к системе.

Требование 3.9.12 Управления информацией Великобритании

В системе, в которой любые карты пациента архивируются (становятся недоступными при нормальном доступе к системе), должна поддерживаться связь между архивированными картами и журналом аудита.

Требование 3.9.13 Управления информацией Великобритании

Необходимо поддерживать ведение истории аудита для включения подробной информации об обновлениях системы, резервном копировании данных и других действиях по обслуживанию системы.

Требование 3.9.14 Управления информацией Великобритании

Поставщики должны гарантировать, что во время обновления системы любые этапы, выполняемые вручную, досрочно зарегистрированы, а любые автоматические этапы включают в себя создание одного или нескольких журналов, которые описывают каждый выполненный этап и включают информацию о том, был ли этап

выполнен успешно. Журналы, содержащие последовательность этапов, должны также указывать информацию о том, была ли общая последовательность этапов выполнена успешно.

Требование 3.9.15 Управления информацией Великобритании

Система должны гарантировать, что входящие и исходящие сообщения отслеживаются таким образом, что информация в журнале аудита содержит полный двухпозиционный вид каждой транзакции для отправленных сообщений и полученных подтверждений и ответов.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)

Регистрация (ведение журнала):

- вход и выход из операционной системы, перезапуск/завершение работы операционной системы;
- регистрация устройств хранения данных со съемным носителем;
- вход и выход из подсистемы защиты, перезапуск/завершение работы подсистемы защиты;
- диагностика и испытание подсистемы защиты;
- обновление подсистемы защиты;
- запуск/остановка и возврат к предыдущему состоянию компонентов подсистемы защиты;
- доступ пользователя к функциям управления подсистемы защиты;
- попытки доступа приложениями к модулям подсистемы защиты;
- печать персональных данных;
- запуск/остановка программ и процессов, предназначенных для обработки защищенных данных;
- попытки доступа к защищенным данным программами и процессами;
- попытки доступа к терминалам, компьютерам, узлам сети, каналам данных, внешним устройствам программами и процессами.

В.16.2 Интерфейс журнала аудита

США

CCHIT SC 02.02

Аудит

Система должна поддерживать ведение журнала в общей библиотеке аудита, используя схему и средства передачи, указанные в спецификации журнала аудита Профиля поддержки аудита доступа и аутентификация узла IHE (ATNA);

NIST SP 800-92/SP 800-92, HITSP T15;

HIPAA 164.312(a) (1); 164.312(b); 164.308 (a) (1) (ii) (A) u (D).

CCHIT SC 02.04

Аудит

Система должна предоставлять авторизованному администратору возможность считывания информации по аудиту из аудиторской документации одним из следующих способов:

1) Система должна предоставлять отчеты таким способом, который позволит пользователю анализировать информацию. Система должна предоставлять возможность создания отчетов на основе интервалов дат и времени сбора отчетов о результатах аудита;

2) Система должна иметь возможность экспорта журналов в текстовый формат таким образом, чтобы обеспечить связь на основе даты и времени (например, синхронизация UTC).

ИСО/МЭК 15408, CC SFR: FAU_GEN;

NIST SP 800-53: AU-3 СОДЕРЖАНИЕ ЗАПИСЕЙ ЖУРНАЛА АУДИТА, AU-10 ОТКАЗОУСТОЙЧИВОСТЬ;

HIPAA: 164.312(b); HITSP/TP15.

В.16.3 Содержание журнала аудита

Канада

Требование безопасности 43 канадской медицинской организации Infoway

Минимальное содержание журналов аудита

Журналы аудита инфоструктуры EHR и журналы аудита систем POS, подключенных к инфоструктуре EHR, должны содержать следующую информацию:

a) идентификатор пользователя, осуществляющего доступ;

b) роль, применяемая пользователем 74;

c) организация пользователя, осуществляющего доступ (по крайней мере в тех случаях, когда лицо осуществляет доступ к информации от имени нескольких организаций);

d) идентификатор пациента субъекта данных (пациент/лицо);

e) функция, выполняемая пользователем, осуществляющим доступ;

f) временная отметка;

g) в случае экстренного доступа к заблокированным или скрытым записям или частям записей причина экстренного доступа в соответствии с выбранной пользователем, осуществляющим доступ, и

h) идентификационная информация лица, ответственного за принятие решений, в случае изменений в директивах согласия, внесенных заместителем лица, ответственного за принятие решений.

Обоснование — Данное требование вытекает из требования конфиденциальности 10 и требования конфиденциальности 15, требования конфиденциальности 19, а также из общепринятой практики обеспечения информационной безопасности.

Великобритания

Требование 3.9.4 Управления информацией Великобритании

Записи журнала аудита должны содержать как минимум следующую информацию:

- идентификационную информацию пользователя. Она включает в себя идентификатор пользователя, имя, ролевой профиль (включая роль и организацию), значения атрибута, полученные из структуры сеанса пользователя;
- идентификационную информацию ответственного лица — лица, осуществляющего ввод или доступ к данным, если он не является пользователем;
- дату и время события;
- подробности о характере события, подвергнутого аудиту, и идентификатор данных (например, ID пациента или ID сообщения), которые связаны с событием, подвергнутым аудиту;
- порядковый номер для защиты от злоумышленных попыток повредить контрольный аудит, например, путем изменения системной даты.

Записи в журнале аудита должны включать подробную информацию об оконечном устройстве (или системе), связанном с записанным действием.

Требование 3.9.2 Управления информацией Великобритании

Данных, которые будут записаны в журналах аудита, должно быть достаточно для того, чтобы следить за тем, используются ли средства контроля доступа по назначению и для выполнения запросов пациентов по получению информации о том, кто осуществлял доступ к их конфиденциальным персональным данным или их персональным данным (например, отображение на экране, распечатка, скачивание) или изменял их, когда и что было отображено на экране или распечатано.

(требование Великобритании для конкретного случая)

Система должна также гарантировать, что хранящиеся журналы аудита записывают информацию обо всех обменах данными с CRS NHS, включая, в частности:

- все попытки использования идентификатора SSO-маркера для осуществления доступа к приложению, включая удачные и неудачные попытки. «Использование маркера» означает вызов SSOTokenManagement API (управление SSO-маркерами) для проверки достоверности маркера;
- все случаи обмена сообщениями — отправка и получение;
- все случаи взаимодействия с SDS Spine.

Такие журналы аудита должны представлять отчет по безопасности для использования в ходе анализа нарушений безопасности и политики, которые могут быть использованы в качестве доказательств при возникновении разногласий. Средства просмотра или восстановление любой личной карты пациента должны использоваться те, которые применялись во все предыдущие дни.

В.16.4 Инструментальные средства анализа журнала аудита

США

CCHIT SC 02.05

Аудит

Система должна предоставлять авторизованному администратору возможность считывания информации по аудиту из аудиторской документации одним из следующих способов:

1) система должна представлять отчеты таким способом, который позволит пользователю анализировать информацию. Система должна предоставлять возможность создания отчетов на основе интервалов дат и времени сбора отчетов о результатах аудита;

2) Система должна иметь возможность экспорта журналов в текстовый формат таким образом, чтобы обеспечить связь со временем (например, синхронизация UTC).

ИСО/МЭК 15408, *CC SFR: FAU_GEN;*

NIST SP 800-53: AU-3 CONTENT OF AUDIT RECORDS, AU-10 NON-REPUDIATION;

HIPAA: 164.312(b); HITSP/TP15.

Канада

Требование безопасности 47 канадской медицинской организации Infoway

Отчет о каждой попытке доступа к EHR пациента/пользователя

Инфоструктура EHR должна идентифицировать всех пользователей, осуществляющих доступ или изменяющих карту определенного пациента/лица за определенный период времени.

Обоснование — Данное требование облегчает обнаружение случаев несанкционированного доступа и помогает в применении последующих мер дисциплинарного или правового воздействия. Следует обратить внимание на то, что уникальные идентификаторы пользователей указаны в требовании безопасности 55.

Требование безопасности 48 канадской медицинской организации Infoway
Сообщение пользователем о каждой попытке доступа
Инфоструктура EHR должна идентифицировать всех пациентов/лиц, к чьим картам был осуществлен доступ или чьи карты были изменены за определенный период времени.
Обоснование — Данное требование значительно облегчает выявление подозрительных или неправомерных случаев использования привилегий доступа.
Уникальные идентификаторы пользователей указаны в требовании безопасности 55.
Требование безопасности 49 канадской медицинской организации Infoway
Анализ журналов аудита инфоструктуры EHR для пациентов/лиц с повышенным риском
Инфоструктура EHR должна предоставлять функции для проведения анализа журналов аудита и контрольных журналов для того, чтобы обеспечить идентификацию всех пользователей, которые изменяли или осуществляли доступ к таким картам (карте) за определенный период времени.
Обоснование — Данное требование облегчает обнаружение случаев несанкционированного доступа и помогает в применении последующих мер дисциплинарного или правового воздействия.
Как отмечалось в требовании конфиденциальности 22а, карты определенных пациентов/лиц (например, политики, знаменитые и известные личности) могут находиться под существенной угрозой осуществления доступа лицами, не имеющими служебной необходимости. Поэтому целесообразно разместить дополнительные средства управления аудитом на этих картах для того, чтобы защитить конфиденциальность пациента. Инфоструктура должна различать эту практическую реальность и способствовать быстрому и регулярному проведению аудита доступа к этим записям (возможно, включая уведомление сотрудника по обеспечению конфиденциальности о каждом доступе).
Данное требование не должно рассматриваться как означающее, что информация в картах такого пациента/лица некоторым образом является более конфиденциальной, чем информация обычных граждан, или что эти карты как информационный ресурс являются более ценными, чем те, риск неприемлемого доступа к которым не повышен. Наоборот, требование гарантирует наличие возможностей для быстрого выявления чрезмерного интереса со стороны пользователей, которые не имеют законной необходимости ознакомления с конфиденциальной информацией.
Для ознакомления с требованиями по обеспечению средств для обозначения пациентов/лиц с повышенным риском см. требование безопасности 22а.
Требование безопасности 46 канадской медицинской организации Infoway
Выявление типов ненадлежащего использования
Инфоструктура EHR должна предоставлять автоматизированные инструменты анализа для содействия аудиторам системы в выявлении и предотвращении ненадлежащего использования системы (например, в сборе данных).
Обоснование — Согласно данному требованию необходимо активно использовать автоматизированные инструменты для поиска несоответствующих типов доступа.
Такое активное обнаружение несанкционированных проникновений является существенным признаком надежности систем безопасности.
В отличие от регистрации аудита инструменты анализа не должны быть доступны постоянно. Достаточно, чтобы такие инструменты были доступны при необходимости. Необходимость будет определяться при разработке системы и соответствующем анализе угроз и рисков.

Великобритания

Требование 3.9.3 Управления информацией Великобритании
Система должна предоставлять средства, позволяющие авторизованным пользователям (например, хранителям Caldicott или специалистам по обеспечению конфиденциальности) просматривать и анализировать журналы аудита, чтобы обеспечить идентификацию всех пользователей системы, которые осуществляли доступ или изменяли карты определенного пациента в течение заданного периода времени (такое изменение включает в себя, например, архивирование карты пациента в системе GP в случаях, когда пациент больше не проходит лечение). Все подобные случаи осуществления доступа также должны быть записаны в соответствующем журнале аудита. Это необходимо для поддержки обязательств, указанных в гарантии медицинской карты.
Такие средства для обеспечения возможности отображения частей журнала аудита основаны на идентификаторе пациента (как правило, это NHS-номер), идентификаторе пользователя, идентификаторе уполномоченного органа, дате и времени, а также порядковом номере.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)
Подсистема журнала аудита должна предоставлять инструменты для просмотра и анализа журнала аудита с возможностью выделения по различным критериям.

B.16.5 Защита журнала аудита

Бразилия

NGS1.08.02
Целостность журнала аудита
Система должна защищать хранимые записи журнала аудита от несанкционированного удаления или изменения.

ABNT NBR ИСО/МЭК 27001:2005, A.10.10.3.
NGS1.08.03
Доступ к журналам аудита
Убедитесь в том, что доступ к журналам аудита предоставлен только пользователям, ответственным за проведение аудита.
ABNT NBR ИСО/МЭК 27001:2005, A.10.10.1.

США

CCHIT SC 02.08
Аудит
Система должна запрещать всем пользователям доступ к чтению записей журнала аудита, за исключением тех пользователей, которые получили явный доступ к чтению. Система должна защищать хранящиеся записи журнала аудита от несанкционированного удаления. Система должна предотвращать внесение изменений в данные журнала аудита.
ИСО/МЭК 15408, *CC SFR: FAU_SAR, FAU_STG;*
NIST SP 800-53: AU-9 ЗАЩИТА ИНФОРМАЦИИ ДЛЯ АУДИТА;
HIPAA: 164.312(a) (1); HITSP/TP15.

Канада

Требование безопасности 50 канадской медицинской организации Infoway
Защита доступа к журналам аудита инфоструктуры EHR
Система EHR должна защитить доступ к записям журнала аудита и должна ограничить доступ к системным инструментам аудита и журналу аудита для того, чтобы предотвратить неправильное использование или несанкционированное разглашение.
Обоснование — Эти требования являются минимальными для поддержания целостности системы и конфиденциальности информации, содержащейся в журнале аудита. Конфиденциальность имеет критическое значение, так как третья сторона, получающая доступа к таким журналам, может вывести ПМД из записей журнала аудита (например, из записи журнала с указанием обновления карты пациента пользователем в центре онкологической помощи можно сделать вывод, что у пациента диагностирован рак).
Требование безопасности 51 канадской медицинской организации Infoway
Обеспечение журналов аудита защитой от несанкционированного вмешательства
Инфоструктура EHR должна обеспечивать соответствующие средства обеспечения безопасности для защиты журналов аудита от несанкционированного вмешательства.
Обоснование — Это требование является минимальным для поддержания целостности системы.

Великобритания

Требование 3.9.6 Управления информацией Великобритании
Система должна гарантировать, что записи в журнале аудита могут быть удалены только привилегированным пользователем при определенных условиях, например, по судебному поручению. Следует отметить, что предполагается, что такие удаления будут очень редкими, и поэтому важно, чтобы доступ к такой функции строго контролировался. Возможность получения таких прав любым локальным пользователем, а также возможность передачи таких прав любым локальным администратором любому локальному пользователю недопустима. Любые попытки обновления или добавления записей в журнале аудита должны быть предотвращены, насколько это возможно.
Требование 3.9.5 Управления информацией Великобритании
Национальный сборник ролей RBAC и действий опубликован в национальной базе данных (NRD) RBAC и описывает действия, применимые к осуществлению доступа к контрольным журналам. Поставщики должны гарантировать, что системы способны на поддержку последних версий вышеуказанного документа. Если поставщики не реализовали национальную модель RBAC, то локальные средства управления доступом должны доказать, что только соответствующие роли могут получить доступ к контрольному журналу.

Российская Федерация

Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 6.2 (необязательное)
Подсистемы журнала аудита должны защищать контрольные журналы от непреднамеренного удаления или изменения. Подсистемы журнала аудита должны осуществлять резервное копирование отдельных частей контрольного журнала.

В.16.6 Хранение журнала аудита

Канада

Требование безопасности 44 канадской медицинской организации Infoway
Хранение журналов аудита
Все организации, размещающие компоненты инфоструктуры EHR или подключенные к инфоструктуре EHR, должны сохранять журнал в течение полного срока хранения записей, прошедших аудит. Это делается для того, чтобы при необходимости обеспечить проведение расследования и предоставить доказательства.
Обоснование — Данное требование вытекает из требования конфиденциальности 19, требования конфиденциальности 20 и требования конфиденциальности 21.

Следует обратить внимание на то, что согласно законодательным актам по медицинской информации провинции Альберта хранителю, разглашающему ПМД, необходимо записывать имя человека, которому хранитель разглашает информацию, дату и цель разглашения, а также описание разглашенной информации. Информация должна сохраняться в течение 10 лет с момента разглашения.

Журналы аудита должны храниться в таком виде, который позволяет проводить анализ информации, содержащейся в журнале. См. требование безопасности 46, требование безопасности 47, требование безопасности 48 и требование безопасности 49.

В.16.7 Управление журналами аудита

См. также ИСО 18308:2011(E) PRS5.1.

США

CCHIT SC 02.01

Аудит

Система должна позволять авторизованному администратору устанавливать добавления и исключения для событий, подвергаемых аудиту в SC 02.03, на основе политики организации и эксплуатационных требований/ограничений.

ИСО/МЭК 15408, CC SFR: FAU_SEL;

HIPAA 164.312(b); 164.308 (a) (1) (ii) (A), (D);

NIST SP 800-53 AU-2 СОБЫТИЯ, ПОДВЕРГАЕМЫЕ АУДИТУ (Оценка, основанная на риске, определяемая организацией) HITSP/TP15.

В.16.8 Постоянное ведение журнала аудита

Канада

Требование безопасности 45 канадской медицинской организации Infoway

Постоянное ведение журнала инфоструктуры EHR

Ведение журнала аудита инфоструктуры EHR должно быть постоянным.

Обоснование — Это требование является минимальными для гарантии того, что ведение журнала не будет прекращено во время работы системы.

Великобритания

Требование 3.9.7 Управления информацией Великобритании

Все контрольные журналы должны быть доступны в любое время, а пользователи не должны иметь никаких средств для отключения любого контрольного журнала.

В.16.9 Восстановление содержания электронной медицинской карты на предшествующий момент времени

Бразилия

NGS1.07.03

Запрет удаления и внесения изменений

Удаление или изменение существующих данных EHR должно быть запрещено. Старые данные должны сохраняться во время выполнения любых корректирующих действий.

Канада

Требование безопасности 39 канадской медицинской организации Infoway

Хранение истории ПМД в инфоструктуре EHR

Инфоструктура EHR должна иметь возможность отображения предыдущего содержания записи на любой момент времени в прошлом, а также возможность отображения связанных данных о том, кто и когда вводил, осуществлял доступ или изменял данные.

Обоснование — Такая возможность позволяет воспроизвести состояние EHR в любой временной точке. Данное требование необходимо для решения ряда задач, включая неосторожные действия и профессиональные дисциплинарные вопросы. Поддержание целостности данных требует такого типа регистрации (ведения журналов). В некоторых юрисдикциях в Канаде пациентам/лицам также разрешается прилагать заявления о несогласии с элементом информации, который пациент считает неправильным (и в случаях, если медицинский работник, который создал данный элемент, с этим не согласен). Инфоструктура EHR должна давать возможность подаче таких заявлений о несогласии, касающихся точности или неточности элемента данных.

Великобритания

Требование 3.9.2 Управления информацией Великобритании

Необходима поддержка средств просмотра и воспроизведения любых личных карт пациента в том виде, в котором они находились ранее.

(См. содержание журнала аудита, приведенное выше, для ознакомления с оставшейся частью требования 3.9.2.)

В.17 Управление версиями программного обеспечения и документация

В.17.1 Управление версиями программного обеспечения

Бразилия

NGS1.01.01

Версия программного обеспечения

Все компоненты EHR-S должны быть идентифицированы и иметь версию программного обеспечения, связанную с отдельной, однозначной ссылкой (уникальный идентификатор, имя, поставщик и номер версии).

EHR должна обладать функциональными возможностями, позволяющими пользователю просматривать версию компонентов их программного обеспечения.
HL7 ERH-S FM IN4.2 ABNT NBR ИСО/МЭК 27001:2005, А.12.5.
См. также требование NGS1.01.03 История изменений.
NGS1.01.02
Исходный код
Номер версии каждого компонента EHR позволяет восстанавливать соответствующие исходные коды для отслеживания исходных файлов, которые их создали.
HL7 ERH-S FM IN5.2 *ABNT NBR* ИСО/МЭК 27001:2005, А.12.5.

В.17.2 Требования к документации

Бразилия

NGS1.09.01
Документация
Справочная документация должна содержать следующую информацию:
- установка системы и требования к системе;
- управление и эксплуатация системы;
- механизмы и методы защиты.

NGS1.09.02
Ссылки на версию ПО в документации
Во всей справочной документации в начале каждого документа должна быть четко обозначена версия, к которой они применяются.
NGS1.09.03
Изменение документации
Следует сообщать об изменениях и хранить историю всех изменений в справочной документации для того, чтобы обеспечивать пользователям возможность проверки всех изменений, внесенных в последнюю доступную версию.
NGS1.09.04
Оператор архива [документация]
Инструкция по установке должна содержать информацию о том, как устанавливать профиль оператора архива для пользователя в SGDB. Дополнительно инструкция по установке должна содержать информацию о том, как устанавливать DBMS SGDB для того, чтобы любой экспорт и восстановление резервных копий данных могли быть выполнены только пользователем, имеющим роль оператора архива.
ABNT NBR ИСО/МЭК 27001:2005.
NGS1.09.05
Ограничение доступа для неавторизованных и неаутентифицированных субъектов [документация]
Инструкция по установке должна содержать информацию о том, как устанавливать DBMS SGDB для того, чтобы аутентификация S-RES и модуль управления доступом предотвращали осуществление доступа неавторизованными и неаутентифицированными субъектами (пользователями или другими системами).
NGS1.09.06
Проверка целостности данных
Инструкция по установке или эксплуатации должна содержать информацию о том, что система должна выполнять проверку целостности данных при создании или восстановлении резервной копии.
NGS1.09.07
Службы, протоколы и установка защиты связи между компонентами
Система должна включать в себя документацию, которая содержит перечень служб (например, PHP, веб-службы) и сетевых протоколов/портов (например, HL-7, HTTP, FTP), которые необходимы для правильной работы и обслуживания системы, в том числе для подтверждения необходимости для этих служб и протоколов. Эта информация может быть использована в медицинском учреждении для правильной настройки своей сетевой защиты (системы сетевой защиты и маршрутизаторов).
Кроме того, инструкция по установке и эксплуатации должна содержать информацию о том, как устанавливать средства защиты связи между компонентами EHR с целью обеспечения безопасности аутентификации, целостности данных и служб защиты конфиденциальности данных.
NGS1.09.08
Синхронизация времени [документация]
Руководство по администрированию и эксплуатации должно предоставлять администратору информацию о том, что часы компонентов EHR должны быть синхронизированы и привязаны к единому и наиболее надежному источнику времени. Руководство также должно предоставлять информацию о том, как выполнять синхронизацию в среде.

ABNT NBR ИСО/МЭК 27001:2005, 10.10.
NGS1.01.05
Зависимости компонентов [документация]
В инструкции по установке и требованиях системы для каждой версии каждого компонента необходимо указать, какими являются зависимости с другими компонентами EHR или компонентами среды, а также требования к эксплуатации. Например, чтобы сообщить, что данная версия компонента совместима со стандартом HL7, версия 2.x (требование к эксплуатации), который использован для данной операционной системы (требование среды), которая зависит от конкретной системы каталогов для аутентификации пользователей.
HL7 ERH-S FM IN5.2.
См. также NGS1.01.03 [документация по управлению версиями ПО].
США
CCHIT SC 04.04
Документация
Система должна включать документированный порядок установки, введения в эксплуатацию и/или подключения продукта.
ИСО/МЭК 15408, *CC SFR: ADO_IGS;*
HIPAA: 164.312(c).
CCHIT SC 04.08
Документация
Система должна включать документацию, которая содержит перечень служб (например, PHP, веб-службы) и сетевых протоколов/портов (например, HL-7, HTTP, FTP), которые необходимы для правильной работы и обслуживания системы, в том числе подтверждение необходимости для этих служб и протоколов. Эта информация может быть использована в медицинском учреждении для правильной настройки своей сетевой защиты (системы сетевой защиты и маршрутизаторов).
ИСО/МЭК 15408, *CC SFR: AGD_ADM;*
NIST SP 800-53 AC-5 CM-6;
NIST SP 800-70;
HIPAA 164.312(a) (1).
CCHIT SC 04.01
Документация
Система должна включать документацию, которая описывает процесс обработки патча (пакета исправлений), который будет использоваться поставщиком для EHR, операционной системы и основных инструментов (например, специальный веб-сайт для уведомления о новых патчах, список утвержденных патчей, особые инструкции по установке и испытанию после установки).
ИСО/МЭК 15408, *CC SFR: AGD_ADM;*
HIPAA: 164.308(a)(5)(i)(B).
CCHIT SC 04.02
Документация
Система должна включать документацию, которая предоставляет пользователям и администраторам объяснение ошибок системы или сообщения с указанием действий, необходимых для их устранения.
ИСО/МЭК 15408, *CC SFR: AGD_ADM;*
HIPAA: 164.312(c).
CCHIT SC 04.03
Документация
Система должна включать документацию о производительности продукта (например, количество пользователей, количество операций в секунду, количество карт, сетевая нагрузка и т. п.) и основных типичных конфигурациях, принятых для такой производительности (например, количество или тип процессоров, конфигурация сервера/рабочей станции и производительность сети и т. п.).
ИСО/МЭК 15408, *CC SFR: AGD_ADM;*
NIST SP 800-53 CM-2;
HIPAA: 164.312(c); 164.306(a)(1).
CCHIT SC 04.06
Документация
Система должна включать документацию, доступную для покупателя, содержащую информацию о том, существуют ли известные проблемы или противоречия со службами безопасности, по крайней мере в следующих областях: антивирусы, обнаружение вторжений, ликвидация вредоносных программ, серверные системы сетевой защиты и разрешение таких конфликтов (например, большинство систем должны учитывать, что полный поиск вирусов должен осуществляться вне периодов максимального использования и должен исключать базы данных).
Канада. Альберта. 7.3.17 (защита);
ИСО/МЭК 15408, *CC SFR: FPT_TST;*

ИСО/МЭК 15408, CC SFR: AGD_ADM;
NIST SP 800-53 SI-3 MALICIOUS CODE PROTECTION;
HIPAA: 164.308(a) (5) (i) (B).
CCHIT SC 04.09
Документация
Система должна включать документацию, которая описывает этапы, необходимые для подтверждения того, что установка системы была завершена надлежащим образом, а система готова к эксплуатации.
ИСО/МЭК 15408, CC SFR: AGD_ADM;
HIPAA: 164.312(e).
CCHIT SC 04.10
Документация
Система должна включать документацию, доступную для покупателя, предоставляющую руководство по конфигурированию и использованию средств контроля защиты, необходимых для поддержания безопасной и надежной работы системы, включая, в частности: создание, изменение и деактивацию учетных записей пользователя, управление ролями, сброс паролей, настройку ограничений пароля и журналы аудита.
ИСО/МЭК 15408, CC SFR: AGD_ADM;
HIPAA: 164.312(a) to 164.312(e).
Российская Федерация
Рекомендация Министерства здравоохранения РФ 2009-12-23, тр. 5.21
Подсистемы безопасности должны быть снабжены документами, в том числе спецификациями подсистемы безопасности и описанием конфигураций компонентов подсистемы безопасности.

B.18 Синхронизация времени и форматирование времени/даты

B.18.1 Формат времени

Бразилия
NGS1.10.1
Единый формат отображения времени для контроля и аудита
Все журналы регистрации времени для контроля и аудита должны иметь одинаковый формат во всей системе EHR.
NGS1.10.2
Формат отображения времени для контроля и аудита в экспортированных журналах
Все журналы регистрации времени для контроля и аудита, найденные в экспортированных журналах, должны быть представлены в формате ИСО 8601:2004, за исключением временных меток, которые соответствуют RFC 3161.
ИСО 8601:2004;
IETF RFC 3161.
США
SC 02.07
Аудит
Система должны обладать способностью форматирования записанных временных меток для экспорта с помощью всемирного скоординированного времени, основанного на ИСО 8601. Пример — «1994-11-05T13:15:30-05:00» соответствует 5 ноября 1994 г., 8:15:30, США, восточное поясное время.
ИСО/МЭК 15408, CC SFR: FPT_STM;
NIST SP 800-53: AU-8 TIME STAMPS; HITSP/TP15;
HIPAA: 164.312(b).

B.18.2 Синхронизация времени

Бразилия
NGS1.10.3
Источник времени
Все журналы регистрации времени для осуществления контроля и аудита по всей системе EHR должны основываться на едином и наиболее надежном источнике времени, установка и доступ к которому может быть осуществлен только менеджером системы.
Система должна указывать в текстовом поле, что является источником времени, и эта информация должна быть проверена пользователями через интерфейс.
ABNT NBR ИСО/МЭК 27001:2005.
США
CCHIT SC 02.06
Аудит
Системы должны поддерживать синхронизацию времени с помощью NTP/SNTP и использовать это синхронизированное время во всех записях безопасности времени.
ИСО/МЭК 15408, CC SFR: FPT_STM;

NIST SP 800-53: AU-8 TIME STAMPS; HITSP/TP16;
HIPAA: 164.312(b).

Великобритания

Требование 3.12.2 Управления информацией Великобритании

Система должна синхронизировать любые внутренние датчики времени со службами сетевого времени, предоставленными NISP, с точностью до 250 мс, используя протокол NTP.

Примечание — Каждая передача сообщений по системам CRS NHS имеет временную отметку, основанную на всемирном координированном времени (GMT). Несмотря на то что приложения могут отображать местное время, временные отметки сообщений должны состоять из значений UTC (GMT).

Требование 3.12.3 Управления информацией Великобритании

Система должна синхронизировать любые внутренние датчики времени с NHSnet/Серверами DNS сети N3 с помощью NTP-протокола.

B.19 Контроль инцидентов нарушения безопасности и конфиденциальности

Бразилия

NGS1.11.01

Интерфейс уведомления

Необходимо предоставить интерфейс, позволяющий пользователям уведомлять о возникновении инцидентов нарушения безопасности, проблемах, улучшениях или выдвигать предложения.

Инфоструктура EHR должна отправлять уведомление ответственному лицу о каждом выявленном типе ненадлежащего использования системы.

ABNT NBR ИСО/МЭК 27002:2005, 13.1.1.

Канада

Требование безопасности 84 канадской медицинской организации Infoway

Сообщения об инцидентах нарушения безопасности, касающихся инфоструктуры EHR

Инфоструктура EHR должна (и всем системам POS, подключенным к инфоструктуре EHR, следует) отправлять уведомление ответственному лицу, описанное в требовании безопасности 3, для каждого выявленного типа ненадлежащего использования системы (см. требование безопасности 46).

Обоснование — Прежде всего решение о том, кто будет являться ответственным лицом, является вопросом управления реализующей организации.

Несмотря на технические требования, устаревшие системы POS могут требовать усовершенствования с помощью административных мер для устранения ограничений производительности для автоматической отправки уведомлений.

B.20 Цифровые сертификаты и цифровые подписи

B.20.1 Использование цифровых сертификатов

Бразилия

NGS2.01.01

Цифровые сертификаты (особые для Бразилии)

Использование цифровых сертификатов, выданных органом по сертификации (АС), аккредитованным Инфраструктурой открытых ключей Бразилии, для аутентификации пользователей и использования цифровых подписей на электронных документах в EHR.

ICP Бразилии; Разрешение CFM (ICP-Brasil; CFM Resolution).

NGS2.01.02

Соответствие с Инфраструктурой открытых ключей Бразилии (особое для Бразилии)

Необходимо соблюдать стандарты по применению, определенные Инфраструктурой открытых ключей Бразилии, при использовании цифровых сертификатов.

ICP-Бразилия; Разрешение CFM (ICP-Brasil; CFM Resolution).

NGS2.04.07

Утверждение Инфраструктуры открытых ключей Бразилии (особое для Бразилии)

Компоненты EHR, использующие цифровые сертификаты для аутентификации, должны быть утверждены Инфраструктурой открытых ключей Бразилии.

B.20.2 Цифровые подписи

Бразилия

NGS2.01.04

Установка корневых сертификатов

Система EHR должны допускать установку набора доверенных корневых сертификатов. Данный набор доверенных корневых сертификатов должен иметь средства контроля защиты.

В.20.3 Предоставление цифровых подписей пользователям

Бразилия

NGS2.02.07

Просмотр информации, требующей подписания

Необходимо обеспечить постоянную возможность просмотра информации, требующей заверения подписью.

NGS2.01.03

Проверка цифровых сертификатов перед использованием

Необходимо осуществить проверку цифрового сертификата перед использованием. Проверка цифрового сертификата включает проверку шифрования и контроль достоверности, включая сертификаты, находящиеся в его цепочке сертификатов. Перед или сразу после использования сертификата система должна проверять, был ли отменен сертификат и его цепочка сертификатов.

Канада

Требование безопасности 79 канадской медицинской организации Infoway

Предоставление цифровых подписей пользователям

Все системы POS, предоставляющие функции, при которых пользователям необходимо использовать электронный аналог собственноручной подписи, должны:

a) позволять пользователям системы применять цифровые подписи, которые отвечают требованиям закона PIPEDA и его правилу 78 для «электронных подписей»;

b) хранить, создавать резервные копии или архивировать цифровые подписи каждый раз, когда осуществляется хранение или архивирование подписанных данных;

c) передавать цифровую подпись каждый раз, когда осуществляется передача подписанных данных, и

d) позволять пользователям подтверждать действительность подписи (т. е. что соответствующий сертификат подписи не был аннулирован) каждый раз при осуществлении доступа к подписанным данным.

Обоснование — Это требование является минимальным для предоставления электронных назначений и других услуг, при которых необходимо использование цифровой подписи. Оно предотвращает секретное, выборочное отображение данных.

Следует обратить внимание на то, что PIPEDA не является единственным законодательным актом в Канаде, разрешающим использование цифровой подписи. Несколько провинций и территорий также приняли закон, позволяющий использовать цифровые подписи там, где ранее требовалось использование собственноручной подписи.

См. также ИСО/МЭК 27002:2005, 12.3.

Великобритания

Требование 3.6.1 Управления информацией Великобритании

Некоторые типы взаимодействия информационных систем требуют использования электронного аналога собственноручной подписи; данное действие по подтверждению содержания выполняется путем использования современных цифровых подписей, основанных на сертификатах, хранящихся на смарт-карте пользователя.

Срочная необходимость в подтверждении содержания, как правило, возникает в области, касающейся выдачи назначений в рамках службы выдачи электронных назначений (EPS) версии 2.

Подробные требования к подтверждению содержания в точке выдачи рецептов (в пределах систем GP) и в точке выдачи препаратов по рецепту (в пределах аптечных систем) предоставляются отдельно в составе основы для обеспечения соответствия EPS версии 2.

В.20.4 Формат подписи

Бразилия

NGS2.02.01

Формат подписи

Следует использовать открытые форматы для обеспечения совместимости данных. Для этого цифровая подпись должна использовать структуры, совместимые с форматом CMS [RFC 3852] или XMLDSIG [RFC 3275].

В.20.5 Проставление цифровой подписи

Бразилия

NGS2.02.02

Проверка назначения цифрового сертификата для цифровой подписи

Перед проставлением цифровой подписи необходимо проверить, имеет ли используемый сертификат функциональное назначение цифровой подписи (цифровая подпись и отказоустойчивость в поле применения ключей).

X.509.

В.20.6 Временные метки

Бразилия

NGS2.02.03

Привязка ко времени для отмены подписи

Все цифровые подписи, введенные в EHR, должны иметь временную метку (RFC 3161), которая должна использоваться в качестве временной ссылки во время проверки аннулирования.

ETSI TS101 733.

В.20.7 Проверка достоверности цифровых подписей

Бразилия

NGS2.02.05

Проверка достоверности цифровых подписей

Следует обеспечить наличие необходимых элементов (информацию о корневых сертификатах, цепочках сертификатов, сертификатов подписи и информацию об аннулировании) для гарантии того, что подлинность цифровой подписи могла быть проверена в любое время в будущем. Данные элементы могут быть включены в реестр с цифровой подписью или приведены в ссылках в данном журнале и сохранены в EHR.

ETSI TS 101 733.

NGS2.02.09

Экспорт подписанных реестров

Все журналы, содержащие цифровую подпись, экспортируемые, например, в другие EHR, должны содержать все необходимые элементы для проверки их достоверности (информацию о корневых сертификатах, цепочках сертификатов, сертификатов подписи и информацию об аннулировании).

Канада

Требование безопасности 80 канадской медицинской организации Infoway

Проверка достоверности и сохранение цифровых подписей ПМД

Каждый раз когда инфоструктура EHR получает данные, содержащие цифровую подпись, которая отвечает требованиям к электронным подписям PIPEDA, инфоструктура EHR должна:

a) по получении подтверждать действительность подписи (т. е. что соответствующий сертификат подписи не был аннулирован);

b) хранить цифровые подписи каждый раз, когда осуществляется хранение, резервное копирование или архивирование подписанных данных;

c) передавать цифровую подпись каждый раз, когда осуществляется передача подписанных данных, и

d) перед передачей подтверждать действительность подписи на момент подписания (например, что соответствующий сертификат подписи не был аннулирован).

Обоснование — Это требование является минимальным для предоставления электронных назначений и других услуг, при которых необходима подпись уполномоченного лица.

См. также ИСО/МЭК 27002:2005, 12.3.

В.20.8 Роль подписывающего лица

Бразилия

NGS2.02.06

Назначение подписи и роль подписывающего лица

Все цифровые подписи должны иметь назначение подписи [атрибут «индикация типа обязательства» (commitment-type-indication)], т. е. тип подтверждения, используемого подписывающим лицом при проставлении цифровой подписи на документе, и роль подписавшего (т. е. атрибут роли подписавшего) в EHR.

ETSI TS 101 733.

В.20.9 Экспорт документов и записей, содержащих электронную подпись

Бразилия

NGS2.02.04

Проверка достоверности цифровой подписи

Для каждой представленной цифровой подписи, включая случаи использования двух или более подписей, система должна проверить достоверность шифрования и проверить аннулирование цифровой подписи (подписей) и цепочки цифровых сертификатов, связанной с каждой подписью.

В.20.10 Политика использования цифровых подписей

Бразилия

NGS2.02.10

Политика использования цифровых подписей

Цифровые подписи в журналах должны быть использованы в соответствии с политикой использования цифровых подписей.

NGS2.02.08

Утверждение ICP Бразилии (особое для Бразилии)

Компоненты EHR, использующие цифровую сертификацию для цифровых сертификатов, должны быть утверждены Инфраструктурой открытых ключей Бразилии.

В.20.11 Использование цифровой подписи на оцифрованных (сканированных) документах

Бразилия

NGS2.04.01

Цифровая подпись ПО

Каждый компонент цифрового преобразования должен иметь пару ключей асимметричной криптосистемы и соответствующий цифровой сертификат. Каждый цифровой документ должен быть подписан компонентом цифрового преобразования посредством этого ключа, используя назначение «подтверждение доставки».

Назначение «подтверждение доставки» может устанавливаться с включением подписанного атрибута «индикация типа подтверждения» (commitment-type-indication) с основным назначением «id-cti-ets-proofOfDelivery», если более конкретное назначение не определено.

NGS2.04.02

Цифровая подпись оператора

Оператор цифрового преобразования должен проставлять цифровую подпись на оцифрованном документе с помощью сертификата Инфраструктуры открытых ключей Бразилии типа А3 или А4, а также с помощью назначения «подтверждение доставки». Назначение «подтверждение доставки» может устанавливаться с включением подписанного атрибута «индикация типа подтверждения» (commitment-type-indication) с основным назначением «id-cti-ets-proofOfDelivery», если более конкретное назначение не определено. Данная подпись должна стоять рядом со встречной подписью программного обеспечения. Оператор должен обязательно проверять кадровую синхронизацию и качество оцифрованного изображения в сравнении с оригиналом, включая возможность повторения процесса оцифровки в случае обнаружения дефектов.

NGS2.04.03

Цифровая подпись ответственного лица

Ответственное лицо должно проставлять цифровую подпись на оцифрованном документе с помощью сертификата Инфраструктуры открытых ключей Бразилии, используя назначение «утверждение». Назначение «утверждение» может устанавливаться с включением подписанного атрибута «индикация типа подтверждения» (commitment-type-indication) с основным назначением «id-cti-ets-proofOfApproval», если более конкретное назначение не определено. Данная подпись должна стоять рядом с встречной подписью программного обеспечения.

NGS2.04.04

Аутентификация

Оператор, ответственное лицо и администратор системы подписей должны быть аутентифицированы в системе в соответствии с NGS2.03.

NGS2.04.05

Время проставления подписи

Каждая подпись на оцифрованном документе должна включать атрибут времени подписания (signing-time attribute), содержащий время проставления подписи в формате UTC.

NGS2.04.06

Кодекс поведения для оцифровки

Необходимо разрешить пользователю выполнять оцифровку только после проставления цифровой подписи в «Кодексе поведения для оцифровки», который должен содержать правила по обеспечению конфиденциальности информации и ответственности за реализацию этого процесса.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам, действующим в качестве национальных

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 17000	IDT	ГОСТ ISO/IEC 17000-2012 «Оценка соответствия. Словарь и общие принципы»
ISO 27799:2008	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[1] ANSI/HL7 EHR R1-2007, The HL7 EHR System Functional Model Release 1 Chapter One Overview, February 12 2007

[2] Brazil Manual Certicacao, SBIS CFM 2009 v3 Conformity Requirements

[3] Canada Health Infoway, Electronic Health Record (EHR) Privacy and Security Requirements, Release 1.1 Montreal November 30, 2004 revised February 7, 2005

[4] Certification Commission for Healthcare Information Technology (CCHIT), Ambulatory Certification Criteria — 2008 Final Criteria Security — Privacy, May 13, 2008

[5] NHS Connecting for Health, Information Governance Requirements for ESP and GPSoC Systems, version 5.0, 17 March 2009

[6] NHS National Programme for Information Technology, Information Governance version 3 — Baseline Index Foundation Module, version 1.0, 30 march 2009

[7] NHS Connecting for Health, CAP Common Assurance Process

[8] EU HITCH project. Healthcare interoperability Testing and Conformance Harmonisation. Available at: http://www.hitch-project.eu/

[9] Central Secretariat ISO Building trust: The Conformity Assessment Toolbox, February 2010

[10] ISO/HL7 10781:2009, Health informatics — Electronic Health Record — System Functional Model R 1.1

[11] ISO/TS 13606-4:2009, Health informatics — Electronic health record communication — Part 4: Security

[12] ISO/TS 14265, Health Informatics — Classification of purposes for processing personal health information

[13] ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[14] ISO/IEC 15408-2, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[15] ISO/IEC 15408-3, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

[16] ISO/IEC 17021:2011, Conformity assessment — Requirements for bodies providing audit and certification of management systems

[17] ISO 18308, Health informatics — Requirements for an electronic health record architecture

[18] ISO/TS 21298, Health informatics — Functional and structural roles

[19] ISO/TS 21547:2010, Health informatics — Security requirements for archiving of electronic health records — Principles

[20] ISO/TR 21548:2010, Health informatics — Security requirements for archiving of electronic health records — Guidelines

[21] ISO/TS 25237, Health informatics — Pseudonymization

[22] ISO 22600-1, Health informatics — Privilege management and access control — Part 1: Overview and policy management

[23] ISO 22600-2, Health informatics — Privilege management and access control — Part 2: Formal models

[24] ISO 22600-3, Health informatics — Privilege management and access control — Part 3: Implementations

[25] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[26] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[27] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[28] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[29] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[30] ISO/CD 27789, Health informatics — Audit trails for electronic health records

[31] Suarez, Walter MD, Overview of Health IT Initiatives in the US: Privacy and Security Standards and Certification Criteria, MPH Director Health IT Strategy, Kaiser Permanente, February 7, 2010

[32] US Government, Federal Register Part III Department of Health and Human Services 45 cfr Part 170 — Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule, July 28, 2010

[33] ISO/IEC 17065, Conformity assessment — Requirements for bodies certifying products, processes and services

УДК 004:61:006.354 ОКС 35.240.80

Ключевые слова: здравоохранение, информатизация здоровья, электронный учет здоровья, требования защиты и конфиденциальности, оценка соответствия

Редактор Д.Е. Титов
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 02.12.2016. Подписано в печать 20.01.2017 Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 11,16. Уч.-изд. л. 10,10. Тираж 26 экз. Зак. 199.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Набрано в ИД «Юриспруденция» 115419, Москва, ул. Орджоникидзе, 11.
www.jurisizdat.ru y-book@mail.ru

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995, Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru