ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57508— 2017/ ISO/TS 14265: 2011

ИНФОРМАТИЗАЦИЯ ЗДОРОВЬЯ

Классификация целей обработки персональной медицинской информации

(ISO/TS 14265:2011, IDT)

Издание официальное

Москва
Стандартинформ
2018

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» (ООО «Корпоративные электронные системы») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава — постоянным представителем ISO/TC 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 июня 2017 г. № 571-ст

4 Настоящий стандарт идентичен международному документу ИСО/ТС 14265:2011 «Информатизация здоровья. Классификация целей обработки персональной медицинской информации» (ISO/TS 14265:2011 «Health informatics — Classification of purposes for processing personal health information», IDT)

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Ноябрь 2018 г.

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 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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАТИЗАЦИЯ ЗДОРОВЬЯ

Классификация целей обработки персональной медицинской информации

Health informatics. Classification of purposes for processing personal health information

Дата введения — 2019—07—01

Введение

Обоснование

Фундаментальный принцип использования персональных медицинских данных состоит в важности знания цели первичного сбора данных, а также того, совпадают ли цели всех последующих действий по обработке этих данных с этой целью или совместимы ли с ней. Применение этого принципа в сочетании со стандартизованным списком целей образует основу принятия решений о совместимости разрешенной цели для различных пользователей, систем, организаций или доменов политик, которым может требоваться общий доступ к персональным медицинским данным.

Стандарты интероперабельности все чаще реализуются в программах развития медицинских информационных систем. Тем самым расширяются возможности обмена медицинскими данными между организациями. Когда это произойдет в достаточно широких масштабах, то большинство решений о запросе медицинских данных будет выполняться автоматически. Чтобы деятельность по обработке данных (сбор, хранение, доступ, анализ, связывание, передача, раскрытие и удерживание) была санкционированной, важно, чтобы политики информационной безопасности, определенные для автоматического применения, сами были интероперабельными. Наличие интероперабельных политик позволит согласованным образом выполнять запросы данных, которыми обмениваются гетерогенные системы и службы. Для определения и ввода в действие автоматически применяемых политик важно иметь средства администрирования, обеспечивающие применение организационного обеспечения, процессов и правил к конструированию информации и информационным технологиям на уровне предприятия и между предприятиями. К таким средствам относятся архитектурные и платформенные решения уровня предприятия, стандарты, стратегии, процедуры, законодательство, нормативные документы, принципы и политики, а также такие средства контроля, как комитеты, бюджеты, планы и соглашения о распределении ответственности (например, соглашения об информационном обмене, соглашения об использовании служб и контракты). Понятно, что не все средства будут применяться автоматически и время от времени потребуется вмешательство человека, обеспечивающее правильное применение политик и средств управления.

По этическим причинам и в соответствии с действующим законодательством обычно требуется, чтобы информация использовалась только для цели ее сбора или создания. Эта цель должна быть явно описана, и на нее должно быть дано согласие. Согласие на использование данных для конкретной цели может подразумеваться, но почти всегда требуется, чтобы цели были объявлены.

Когда данные предназначены также для других и отличающихся целей, то может требоваться новое согласие на новую цель. Например, в некоторых юрисдикциях данные, собранные для цели оказания медицинской помощи, не могут быть автоматически, без получения нового согласия, использованы для научных целей. Это же относится и к применению информации, собранной для научных целей, в процессе оказания медицинской помощи. Знание цели доступа к информации существенно для принятия решения о том, можно ли разрешить такой доступ.

Издание официальное

Таким образом, проблема состоит не только в определении, имеет ли пользователь разрешение на доступ к конкретным элементам данных, но еще и в том, имеет ли он разрешение на доступ с определенной целью. Поэтому существенно знать, что контекст, в котором объявлены доступ и использование, является правильным. Когда цель (или использование, цель использования, контекст использования) точно определена, это помогает определить, что доступ к защищаемым элементам информации разрешен авторизованным пользователям в соответствии с конкретной, подходящей и однозначно трактуемой политикой. Явное объявление предполагаемой цели использования перед получением разрешения на доступ помогает также гарантировать, что пользователи информированы о том, что такое разрешение не подразумевает использования данных в иных, не декларированных или несовместимых целях. Знание цели использования помогает внести ясность в ситуациях, когда существует несколько потенциально конфликтующих контекстно-чувствительных политик разрешения одного и того же доступа к идентичным элементам информации.

Предыстория

Общий архитектурный подход к службам применения политик и формальному определению политик описан в ИСО/ТС 22600-1. Однако, как и в случае других общих архитектур, для обеспечения интероперабельности политик необходима конкретизация общего подхода. При описании области применения политик необходимо также указать, какие свойства информации должны приниматься во внимание при принятии решений о доступе. Требуется также описать высокоуровневую модель политик, учитывающих эти свойства, которой должны соответствовать все экземпляры политик этого типа.

В ИСО/ТС 13606-4 такая модель политик описана для одного конкретного случая, а именно для запроса и предоставления выписок из электронной медицинской карты (ЭМК).

Даже если несколько сторон согласовали общую модель политики, этого недостаточно для отображения политик (автоматического преобразования политик одной стороны в политики другой стороны): термины, в которых описано каждое свойство в общей модели политик, должны быть взаимно понятны потребителям и поставщикам медицинской информации. Другими словами, чтобы автоматически принимать решение о доступе, свойства и термины, использованные поставщиком в политике получения (сбора) информации, должны иметь вычисляемое соответствие терминам и политикам раскрытия информации ее потребителем.

По историческим причинам использование данных классифицируется как первичное и вторичное. Поскольку эти термины связаны, они приобретают смысл только в том случае, когда поставщику данных известны намерения их потребителя. Доказать, что некоторые цели использования важнее других, не всегда просто, и может оказаться, что вторичное использование данных в целях благосостояния общества является важной целью. Поэтому предлагается заменить эти термины явными и нейтральными, но информативными категориями. Данные, включаемые в ЭМК, изначально собираются для целей оказания медицинской помощи, хотя затем могут использоваться для других целей. Явное указание этих целей вместо общей характеристики «вторичное использование» улучшит информационное взаимодействие, прозрачность и правильность использования данных.

Настоящий стандарт служит семантическим дополнением ISO/TS 22600-1 и ISO/TS 13606-4, которые предоставляют формальные архитектурные и моделируемые описания политик, но не содержат словарь целей использования. Однако при этом не требуется, чтобы уполномоченный орган принял какой-либо из этих двух стандартов, чтобы ввести в действие классификацию целей, предложенную в настоящем стандарте.

Существуют другие стандарты, определяющие словари, которые предназначены для обеспечения интероперабельности и могут использоваться при конкретизации политик. В ISO/TS 13606-4 определены словари категорий чувствительности медицинских данных и функциональных ролей. В ISO/TS 1298 определен словарь структурных ролей (и воспроизведен словарь функциональных ролей из ISO/TS 13606-4). В ИСО 10181-3 предложено определение информации контроля доступа ACI (access control information), существенное для определения политики контроля доступа.

Контекст определения целей использования данных

Определение целей использования данных является первым критичным шагом в цепочке действий по сбору данных и различной обработки этих данных. Только в том случае, когда цель использования данных известна, можно оценить, являются ли доступ к данным или другая деятельность по их обработке допустимыми, например:

- какие именно данные допускается собирать;
- как их следует использовать,
- кому их следует раскрывать;
- в течение какого времени они должны быть доступны.

При принятии решения о предоставлении доступа авторизация представляет собой отдельную ось по отношению к цели использования и поэтому не должна включаться в данную классификацию. Правила авторизации сбора, использования и раскрытия будут различными в разных юрисдикциях, странах или ситуациях и будут зависеть от среды использования данных. Авторизация может быть представлена разными способами, например в соответствии с информированным согласием, по закону, в соответствии с политикой. В любой конкретной среде для разрешения различных видов использования могут требоваться разные уполномоченные органы. Например, для использования данных в научных целях может требоваться явное согласие лица, а использование данных при непосредственном оказании медицинской помощи может быть основано на подразумеваемом согласии. Для использования данных следственными органами может требоваться решение суда, разрешающее раскрытие и сбор этих данных. Авторизация обеспечивает дополнительный контроль сбора или раскрытия данных для их использования (несанкционированный сбор, использование или раскрытие данных могут создавать пользователю юридические или иные риски).

Первоначальный сбор или создание данных преследуют некоторые цели, которые должны быть определены и явно названы, если только эти действия не совершаются по хорошо известным основаниям и их цели очевидно вытекают из контекста сбора, и при этом предполагается, что субъект данных адекватно осознает это (например, если существует подразумеваемое информированное согласие, основанное на том, что субъект знает или должен знать). Впоследствии, когда данные затребованы организацией или группой лиц либо раскрыты для использования внешними сторонами, потребитель полученных данных может преследовать другую цель. В юрисдикциях, где новая или дополнительная цель разрешается (в тех случаях, когда новая цель использования данных возникла после их сбора), может потребоваться сопоставление новой цели с ранее авторизованной, чтобы принять решение о ее допустимости.

В юрисдикциях, где разрешено использование данных, собранных для одной цели, для другой цели может потребоваться сопоставление двух целей (первоначальной, разрешенной в соответствии с согласием или иной авторизацией, и новой целью доступа к данным или их раскрытия), чтобы принять решение о допустимости новой цели.

После совершения доступа к данным, предназначенным для определенной цели доступа или раскрытия, может потребоваться регистрация этой цели в журнале доступа. Это справедливо и в том случае, если доступ осуществляется по закону: все равно должна быть объявленная и документированная цель.

У той стороны, которой требуются данные, должна существовать определенная цель. При некоторых обстоятельствах, имеющих место, например при выполнении следственных действий, запрашивающая сторона может иметь полномочия не объявлять цель запроса данных.

Сбор данных, осуществляемый непосредственно каким-либо лицом или косвенно некоторым органом, следует ограничивать той информацией, которая должна удовлетворять дозволенным потребностям собирающей стороны («ограничение сбора данных»). Описание дозволенных потребностей является частью высокоуровневой политики организации или юрисдикции и управления ее применением.

Определенная цель также обозначает контекст получения информированного согласия, являющегося механизмом, с помощью которого лицо способно контролировать сбор, использование и/или раскрытие его данных; важно, чтобы механизм согласия позволял субъекту данных делать свободный и информированный выбор. Оборот «даю информированное добровольное согласие» подразумевает право субъекта знать о том, как будут использоваться его данные после сбора.

В некоторых случаях, например, когда данные собираются для целей, определенных законом, после раскрытия данные могут использоваться для любой из этих целей, например для проведения следственных действий. Независимо от того, раскрыты ли данные в соответствии с требованиями закона или по соглашению, раскрывающая сторона обладает юридическими правами на это действие. Однако при этом может требоваться, чтобы данные раскрывались только для определенной цели.

В настоящем стандарте определены категории целей использования данных, но список этих категорий не является исчерпывающим для описания юридических обязательств, возникающих при раскрытии данных. Юридические обязательства, возникающие при раскрытии, предоставлении или передачи данных, перекрывают требования совпадения цели, для которых данные удерживаются, с целями их

использования получателем. Получателю юридически разрешено запрашивать и получать информацию, не объявляя цель использования, не объявляя ее совпадение с существующими целями и не получая согласия на удерживание данных.

Иногда может оказаться важным применять политики к получателю раскрываемых данных (косвенному сборщику), чтобы гарантировать использование им данных только для декларированной цели. Выполнение требований закона или политики можно обеспечить на техническом уровне, используя контроль доступа на основе категорирования данных или средств управления ими.

Для целей использования или специфичного использования может требоваться, а может и не требоваться идентификация субъекта данных. Для некоторых целей могут требоваться идентифицируемые, деперсонифицированные, обезличенные, псевдонимизированные или агрегированные данные. Хотя настоящий стандарт не содержит требований к тому, для каких целей могут требоваться или не требоваться идентифицируемые данные, из общих соображений понятно, что в тех случаях, когда идентификация субъекта данных не требуется, ее раскрывать не следует. Идентификация чаще всего требуется, если использование данных осуществляется в пользу конкретного субъекта данных, например, когда субъект данных является также субъектом медицинской помощи. Деперсонификация, обезличивание или псевдонимизация могут применяться для обеспечения конфиденциальности персональных данных или как условие, которое уполномоченные органы накладывают на процессы сбора, использования или раскрытия данных. В свою очередь, это означает, что точно так же, как требование деперсонификации может быть условием использования данных, конкретная цель использования данных может быть требованием, накладываемым на использование даже деперсонифицированных или обезличенных данных в соответствии с политикой или законодательством, принятым в данной юрисдикции.

Если для обеспечения связи с другими источниками данных должен присваиваться уникальный идентификатор, то на практике хорошо себя зарекомендовали истинные псевдоидентификаторы, хотя в тех случаях, когда надежный механизм присваивания псевдоидентификаторов отсутствует, для связи с другими источниками данных нередко используются идентифицирующие данные. Основа управления псевдоидентификаторами изложена в ISO/TS 25237.

Отчетность сама по себе не является отдельной категорией использования данных, скорее таким использованием данных, целью которого является цель предоставления отчетности, которая может быть предписана или авторизована государственным органом. Следовательно, отчетность является законным раскрытием или использованием данных, но при этом важно определить цель использования данных, а не просто констатировать, что данные раскрыты (в форме отчета) конкретным потребителям. Если для связывания содержания отчета с другими источниками информации требуются идентифицирующие данные, чтобы определить, какие записи относятся к одним и тем же лицам, то целью использования является причина связывания.

Предлагаемая классификация целей может использоваться в сочетании с функциональными ролями и категориями чувствительности данных для дополнения политики и заполнения ее дополнительных частей. При автоматизированной обработке можно конфигурировать шаблоны реализации, используя цели в процессах автоматизированного принятия решений и рабочих процессах, а также подстраивать цели к положениям действующего законодательства, стандартов и нормативных актов профессиональной деятельности. Например, организация может использовать следующие сочетания конкретных целей:

- определить политику укрепления здоровья;
- обеспечить эффективное управление здравоохранением;
- обратить внимание общественности на факторы, влияющие на здоровье;
- под общим названием «использование системы здравоохранения» или «планирование системы здравоохранения». При этом конкретные цели сбора данных, осуществляемого организацией, всегда выбираются из того же самого ограниченного множества целей использования.

Не всегда конкретная группа целей, с которыми организация собирает отдельные данные, может распространяться на массовый сбор данных. Например, организация здравоохранения не может предполагать, что данные, собранные в процессе непосредственного оказания медицинской помощи, могут быть использованы для научных исследований или маркетинга и считать эти цели совместимыми, даже если она вовлечена во все эти виды деятельности.

В настоящем стандарте не делаются никакие утверждения о конкретной частоте или масштабе контроля соответствия цели использования информации ее получателем с целями хранения данных. Однако в нем утверждается, что каждый доступ должен осуществляться в соответствии с согласованными

политиками, описывающими в том числе совместимость целей. Такая совместимость может проверяться при каждом запросе данных к дискретным вычислительным службам, или разово в каждом сеансе пользователя, или при передаче пакета данных в конкретную зону. Например, внешняя служба обработки счетов на оплату лечения может иметь разрешение только на обработку счетов, а любое другое использование данных будет считаться нарушением контракта. В этом случае зона использования данных имеет единственную цель использования, и проверка соответствия этой цели может осуществляться однократно при каждой передаче пакета счетов, а не для каждого отдельного счета, входящего в пакет. Частота опроса служб политик должна определяться в зависимости от того, применяются ли политики к отдельным транзакциям или пакетам транзакций. Таким образом, точка применения политик (policy enforcement point) не должна обращаться к точке принятия решений (policy decision point) или вычислять цель использования для каждой записи. Политика прежде всего является административным решением, являющимся частью процесса управления, использующим машину применения политик для автоматизации принятия решения о доступе в зоне, где цель использования данных, скорее всего, предопределена. В настоящем стандарте не подразумевается никакой конкретный технический метод реализации служб политик или проверки политик. Однако такие заранее заданные или предопределенные цели использования могут проверяться строго применяемыми средствами, совместимыми с политиками, только при наличии интероперабельных спецификаций политик, включающих в себя в том числе совместимый словарь.

1 Область применения

Настоящий стандарт определяет совокупность высокоуровневых категорий целей обработки персональной медицинской информации (ПМИ) (то есть сбора, использования, хранения, доступа, анализа, создания, связывания, передачи, раскрытия или удерживания), которая может служить платформой, используемой для классификации различных конкретных целей, определяемых областями применения политик (например, организациями здравоохранения, региональными органами управления здравоохранением, юрисдикциями, странами), а также для согласованного управления информацией при оказании медицинской помощи и при передаче записей электронных медицинских карт, пересекающей границы организаций и юрисдикций.

Область применения настоящего стандарта ограничена ПМИ, определенной в ИСО 27799 как информация об идентифицируемом лице, связанной с его физическим или психическим здоровьем или с предоставлением ему медицинской помощи. Такая информация может включать в себя:

- сведения о регистрации лица для оказания ему медицинской помощи;
- сведения о платежах за медицинскую помощь, оказанную лицу, или о его медицинском страховании;
- число, символ или конкретный код, присвоенные лицу для уникальной идентификации при оказании медицинской помощи;
- любые сведения о лице, собранные в процессе оказания ему медицинской помощи;
- информацию, произведенную при обследовании части тела или исследовании телесной субстанции;
- идентификацию лица, например медицинского работника, как поставщика медицинской помощи данному лицу.

Настоящий стандарт определяет не исчерпывающий перечень целей обработки этой информации, а общий список, на который могут быть отображены различные национальные списки целей, и тем самым способствует автоматизированной авторизованной трансграничной передаче содержания ЭМК.

Настоящий стандарт не предназначен для контроля использования неперсонифицированной медицинской информации. Но в связи с тем, что обезличивание или деперсонификация данных могут быть условием дальнейшего или нового использования, определенная цель использования данных может служить требованием даже для обработки деперсонифицированных или обезличенных данных, предъявляемым политикой или законодательством в данной юрисдикции.

Медицинские данные, которые были необратимо деперсонифицированы, формально не входят в область применения настоящего стандарта. Но поскольку процессы деперсонификации нередко имеют некоторую степень обратимости, настоящий стандарт может применяться и к раскрытию деперсонифицированных медицинских данных, если это будет сочтено целесообразным.

2 Термины и определения

Для целей настоящего стандарта применяются приведенные ниже термины и определения:

2.1

контроль доступа (access control): Предотвращение неавторизованного доступа к ресурсу, включая предотвращение использования ресурсов неавторизованными способами.

[ИСО 7498-2:1989, определение 3.3.1]

2.2

регистрационный журнал (audit trail): Хронологическая регистрация действий пользователей информационной системы, обеспечивающая возможность достоверного восстановления предыдущих состояний информации.

[ИСО 13606-1:2008, определение 3.9]

2.3 **авторизация** (authorization): Разрешение выполнять определенные операции или использовать определенные методы либо службы.

2.4

медицинская информация (clinical information): Информация о лице, относящаяся к его здоровью или лечению.

[ИСО 13606-1:2008, определение 3.13]

2.5

конфиденциальность (confidentiality): Процесс, гарантирующий, что информация не доступна или не раскрыта неавторизованным субъектам, сущностям или процессам.

Примечание — Адаптированное определение из ISO/TS 13606-4:2009.

2.6 **согласие** (consent): Добровольное информированное согласие субъекта на обработку его персональных данных.

2.7 **собранные** (collected): Полученные и сохраненные.

2.8 **уничтожение данных** (data destruction): Операция, в результате которой информация о субъекте необратимо удаляется из памяти или хранилища без возможности восстановления.

Пример — Уничтожение данных может осуществляться с помощью многократной перезаписи последовательностями случайных битов.

2.9

защита данных (data protection): Техническая и социальная система мероприятий по согласованию, управлению и обеспечению неприкосновенности, конфиденциальности и защиты информации.

[ISO/TS 25237:2008, определение 3.15]

2.10 **субъект данных** (data subject): Идентифицированное или идентифицируемое физическое лицо, являющееся субъектом персональных данных.

2.11 **использование данных** (data use): Обработка или применение данных для конкретной цели.

Примечание — Сюда относится воспроизведение информации, но не ее раскрытие.

2.12

деперсонификация (de-identification): Общее название любого процесса удаления связи между совокупностью идентифицирующих данных и субъектом данных.

[ISO/TS 25237:2008, definition 3.18]

2.13 **раскрыть** (disclose): Предоставить данные тем, кто обычно не авторизован их иметь.

2.14 **экстренный доступ** (emergency access): Доступ к данным с допустимой конкретной целью в случае угрозы здоровью или жизни лица, требующий особых полномочий или отмены других ограничений для срочного и бесперебойного получения информации.

2.15

явное согласие (explicit consent, express consent): Непосредственно данное добровольное разрешение, выраженное устно или письменно.

Примечание — Адаптированное определение из ИСО 18308:2011.

2.16 **подразумеваемое согласие** (implied consent): Произвольное соглашение о том, что делается или предлагается, которое может быть обоснованно выведено из действия или бездействия субъекта данных.

2.17

управление информацией (information governance): Процессы, посредством которых организация получает гарантию того, что риски для ее информации, а потому и работоспособность и целостность организации эффективно идентифицируются и управляются.

[ИСО 27799:2008, определение 3.2.8]

2.18 **информированное согласие** (informed consent): Согласие, данное на основе знания.

2.19 **постоянный** (persisted): Хранящийся на постоянной основе.

2.20

политика (policy): Комплекс юридических, методических, организационных, функциональных и технических обязательств по обмену информацией и совместной деятельности.

[ISO/TS 22600-1:2006, определение 2.13]

2.21

соглашение о политике (policy agreement): Письменное соглашение, в котором все участвующие стороны обязуются придерживаться определенного комплекса политик.

[ISO/TS 22600-1:2006, определение 2.14]

2.22

конфиденциальность (privacy): Защита от вмешательства в личную жизнь или личные дела, выраженного в излишнем или неправомерном сборе и использовании персональных данных.

[ИСО/МЭК 2382-8:1998, определение 08-01-23]

2.23

обработка (processing): Получение, запись, сохранение, изменение, извлечение, уничтожение или раскрытие данных.

[UK Data Protection Act: 1998]

3 Сокращения

ОИД — объектный идентификатор (OID, Object Identifier).

ЭМК — электронная медицинская карта (EHR, Electronic Health Record).

4 Соответствие

Домен политик соответствует настоящему стандарту, если каждая согласованная цель обработки ПМИ, разрешенная в этом домене, опубликована в такой форме, которая позволяет отнести ее к одной из категорий, описанных в разделе 6. При этом не требуется, чтобы каждой категории целей, определенных в настоящем стандарте, соответствовала цель, поддерживаемая в таком домене политик.

5 Контекст

Контекст применения настоящего стандарта детализируется следующим образом:

- при определении целей важно рассматривать все действия обработки: сбор, хранение, доступ, анализ, связывание, передачу, раскрытие и удерживание;
- чтобы субъекты данных могли осуществлять добровольный информированный выбор, цели обработки данных должны быть заявлены при сборе данных или до его начала, при этом должны быть названы все предполагаемые цели;
- раскрывающая сторона, будь то физическое лицо, другая организация или государственный орган, обязана иметь эту информацию, чтобы контролировать потребности в сборе данных и ограничивать этот сбор;
- должны предоставляться точные объяснения целей обработки данных, описания необходимости их сбора и последующего использования;
- связывание означает задачу поиска записей, относящихся к одной и той же сущности, в двух файлах или более либо базах данных. Связывание записей может осуществляться с помощью соединения наборов данных, не имеющих общего ключа; наборы данных, к которым применена процедура связывания записей, называются связанными. Связывание представляет собой способ подготовки данных к использованию, но, подобно сбору, доступу и раскрытию, не является собственно использованием. Связывание может быть разрешено или запрещено, поэтому его можно рассматривать как условие использования;
- цели использования определяют, как будет осуществляться управление данными, а именно: какие данные следует собирать, как они будут использоваться, раскрываться и удерживаться, как должно быть реализовано получение согласия, насколько точным оно должно быть, какая рекомендуется степень защиты;
- идентификация целей необходима для ответственного управления информацией. Может требоваться документирование целей для выполнения этических и юридических требований к прозрачности;
- цели должны быть названы ясно и конкретно; не следует давать настолько широкие определения, что они потеряют смысл;
- чтобы цели были понятными при информационном взаимодействии сторон и юрисдикций, объявления целей должны быть представлены интероперабельным способом;
- описания целей должны предоставлять субъекту медицинской помощи или его законному представителю знание, необходимое для принятия решения о согласии или регистрации;
- персонал должен проявлять инициативу в разъяснении целей субъекту медицинской помощи или его законному представителю, а не дожидаться их вопросов;
- описания целей должны содержать краткие сведения о мерах защиты, раскрытии информации, авторизации сбора данных и контролирующих органах. Более подробные сведения должны предоставляться по запросу;
- субъект медицинской помощи или его законный представитель могут уведомляться о целях устно или письменно. При устном уведомлении может быть полезным документирование факта уведомления;
- сведения о целях следует передавать всем тем сотрудникам организации, кто будет иметь доступ к данным или использовать данные. Эти же сведения следует включать в учебные курсы по допустимому использованию данных;
- в строго определенных ситуациях ограничения доступа к данным, вытекающие из целей использования или информированного согласия, могут отменяться. Такая отмена может быть основана на политике, требованиях этики, положениях законодательства и осуществляться с помощью средств, обеспечивающих экстренный доступ в экстренных ситуациях. Примером ситуаций, когда доступ необходим для других целей и осуществляется с согласия или без согласия субъекта данных, могут служить осуществление правосудия и исполнение судебных актов, ликвидация вспышки инфекционного заболевания. При создании механизмов отмены ограничений следует рассматривать ряд факторов, в том числе роль пользователя, исходную цель использования, предполагаемую новую цель, экстренность ситуации, риск причинения вреда субъекту данных, другому лицу или обществу в целом;
- существуют ситуации, при которых возникают угрозы здоровью или жизни лица. При оказании экстренной медицинской помощи этому или другому лицу могут потребоваться данные, первоначальная цель сбора которых не связана с оказанием медицинской помощи. Хотя запрет на использование этих данных для новой цели или ограничения, наложенные документом согласия, могут быть сняты,

существуют некоторые цели использования, для которых экстренность не может иметь место и, следовательно, экстренный доступ не может быть предоставлен. Примерами могут служить обучение и научная работа;

- важно тщательное конструирование механизмов экстренного доступа или снятия ограничений на цель использования. В таких механизмах предусматривается регистрация исходной цели, новой цели, идентификации пользователя и его роли, а также данных, требуемых в экстренных ситуациях. Это позволит регистрировать в журнале экстренный доступ в целях выполнения требований закона и политики о предоставлении отчета по снятию ограничений организации, ответственной за данные и субъект данных. Однако соображения безопасности пациента означают, что такие механизмы снятия не должны препятствовать доступу к данным, необходимым в экстренных ситуациях.

6 Терминология классификации целей обработки персональной медицинской информации

В таблице представлены кодируемые значения, термины классификации и описания целей обработки ПМИ. Для идентификации этого словаря кодированных целей должен использоваться следующий ОИД: ИСО (1) стандарт (0) классификация целей обработки медицинской информации (14265) терминология классификации целей обработки ПМИ (1).

Таблица 1 — Коды, термины классификации и описания целей

Код цели	Термин классификации	Описание (справочное)
1	Оказание медицинской помощи отдельному субъекту	Информирование лиц или процессов, ответственных за предоставление медицинской помощи ее субъекту
2	Оказание экстренной медицинской помощи отдельному субъекту	Информирование лиц, ответственных за оказание экстренной медицинской помощи субъекту. В отличие от цели 1, может требоваться применение политики отмены ограничений, накладываемых согласием
3	Обеспечение деятельности по оказанию медицинской помощи отдельному субъекту, осуществляемой внутри организации	Информирование лиц или процессов, обеспечивающих деятельность других лиц по оказанию медицинской помощи ее субъекту, путем координации действий этих лиц или подразделений
4	Обеспечение оплаты медицинской помощи, оказанной отдельному субъекту	Информирование лиц или процессов, обеспечивающих доступность денежных средств и/или получение разрешений плательщиков на оказание медицинской помощи ее субъекту
5	Управление организацией оказания медицинской помощи и контроль ее качества	Информирование лиц или процессов, ответственных за обеспечение доступности, качества, безопасности, равных условий медицинской помощи и эффективность затрат на нее
6	Обучение	Обеспечение обучения и повышения профессиональной квалификации медицинских работников
7	Санитарно-эпидемиологический контроль	Информирование лиц или процессов, ответственных за мониторинг значимых событий общественного здоровья и организацию медицинской помощи, необходимой для лечения или профилактики заболеваний
8	Экстренные санитарно-эпидемиологические мероприятия	Информирование лиц, ответственных за ликвидацию существенных угроз общественному здоровью. В отличие от цели 7 может требоваться применение политики отмены ограничений, накладываемых согласием
9	Управление организацией здравоохранения	Информирование лиц или процессов, ответственных за мониторинг здоровья населения и оказания медицинской помощи, для планирования ресурсов медицинской помощи и стратегии их развития
10	Научные исследования	Обеспечение создания обобщенных знаний

Окончание таблицы 1

Код цели	Термин классификации	Описание (справочное)
11	Маркетинговые исследования	Обеспечение создания знаний, специфичных для анализа обращения лекарственных средств и деятельности организаций здравоохранения
12	Юридическая процедура	Информирование лиц или процессов, ответственных за применение законодательства, осуществление правосудия и исполнение судебных актов, контроль лицензируемой деятельности
13	Использование субъектом медицинской помощи	Информирование субъекта медицинской помощи либо его законного представителя, обеспечивающее его права на получение медицинской помощи или, в случае смерти лица, права члена его семьи
14	Неуточненная	Раскрытие на основе авторизации, не требующее объявления цели, или цели, которые не могут быть отнесены к другим категориям

Приложение А
(справочное)

Примеры

А.1 Общие сведения

В настоящем приложении приведен ряд примеров, иллюстрирующих каждую категорию целей, определенных в разделе 6. Эти примеры не обладают большой полнотой, они предназначены только для пояснения назначения терминов целей. В конкретной юрисдикции может оказаться, что различным условиям использования могут быть сопоставлены более детальные категории целей. Отличия в условиях использования могут быть обусловлены политиками, являющимися более или менее ограничивающими, например для экстренной помощи может не требоваться тот же уровень согласия, как для плановой помощи. Такие отличия обусловлены средствами управления информацией и политиками информационной безопасности, используемыми в юрисдикциях, где осуществляется транзакция.

А.2 Оказание медицинской помощи отдельному субъекту

Использование информации с этой целью может принести субъекту медицинской помощи непосредственную пользу, оправдывающую раскрытие и использование идентифицирующих его данных. Следующий уровень детализации этой категории использования важен для описания деловых требований.

Эта категория цели может возникать при выполнении следующих действий:

- информирование о непосредственном оказании медицинской помощи медицинским работником;
- поиск семейного анамнеза, например для его переноса из медицинской карты одного члена семьи в медицинскую карту другого члена.

Примечание — Обычно такая операция рассматривается как вторичное использование, на которое должно быть получено согласие того лица, к кому эта информация относится. Необходимо отличать использование данных лица для непосредственной пользы этому же лицу от использование этих данных в пользу другого лица и учитывать возможную необходимость авторизации такой операции и выполнения других условий;

- формальная регистрация действий по оказанию медицинской помощи и принятию решений;
- информирование и санитарное просвещение субъекта медицинской помощи либо законного представителя, действующего от его имени;
- обеспечение взаимодействия медицинских работников, например направление к другому врачу, консультирование, получение других мнений;
- анализ записей в медицинскую карту, например для просмотра диагнозов пациента, мониторинга планируемых действий и отклонений от ожидаемой динамики;
- разбор случая оказания медицинской помощи субъекту данных, осуществляемый, например, в консилиуме или на врачебной конференции;
- информационное обеспечение принятия медицинских решений, например автоматическая проверка предосторожностей или противопоказаний;
- обеспечение управления планом ведения субъекта данных, включая контроль перехода к следующему этапу, повторные приглашения на скрининговые обследования, корректировку плана при наличии просроченных мероприятий, анализ отклонений;
- отслеживание странных происшествий с пациентом.

А.3 Оказание экстренной медицинской помощи отдельному субъекту

Использование информации с этой целью осуществляется в случаях, когда субъекту необходима экстренная медицинская помощь. При этом возможна ситуация, когда доступ, разрешаемый при оказании плановой медицинской помощи, не может быть предоставлен.

Эта категория цели может возникать при выполнении следующих действий:

- информирование об экстренном непосредственном оказании медицинской помощи стороной с правом оказания медицинской помощи, возможно, вне организации здравоохранения;
- информирование об экстренном непосредственном оказании медицинской помощи по обстановке, например врачом, оказавшимся вблизи с пациентом в бессознательном состоянии, но не имеющим иных причин доступа к его ПМИ.

А.4 Обеспечение деятельности по оказанию медицинской помощи отдельному субъекту, осуществляемой внутри организации

Использование информации с этой целью осуществляется в случаях, когда раскрытие и обработка информации необходимы для координации медицинской помощи или выделения ресурсов. Эта категория цели может возникать при выполнении следующих действий:

- обеспечение работы непосредственного поставщика медицинской помощи другими подразделениями организации, например лабораторией;
- подготовка направлений и эпикризов для передачи другому подразделению организации;
- обеспечение координации медицинского помощи, например с помощью записи на прием;
- активный поиск субъектов медицинской помощи, пропустивших очередное получение медицинской услуги или программы оздоровления;
- оценка состояния здоровья субъекта медицинской помощи и рисков, например в медицинских отчетах, счетах на оплату лечения, приложениях медицинского страхования;
- проверка наличия разрешений на донорство органов и тканей, а также пригодности к донорству.

А.5 Обеспечение оплаты медицинской помощи, оказанной отдельному субъекту

Данные этой категории персонифицированы и могут иметь высокую чувствительность. Поэтому на их использование могут накладываться те же ограничения законодательства и политик, что и на персонифицированные данные, используемые при непосредственном оказании медицинской помощи.

Эта категория цели может возникать при выполнении следующих действий:
- подготовка требования на возмещение затрат, направляемого государственным или частным организациям (например, счетов на оплату услуг, счетов, выставляемых страховой медицинской организации);
- обеспечение оплаты (например, получение информации о номерах кредитных карт и других данных, связанных с платежами);
- обеспечение взаимодействия с государственными программами медицинского страхования, включая учет фиксированных выплат и управление объемами медицинской помощи;
- информирование об авторизации лечебно-профилактических мероприятий, например получение разрешения на конкретный вид лечения.

А.6 Управление организацией оказания медицинской помощи и контроль ее качества

Использование информации с этой целью осуществляется при управлении доступностью, качеством и безопасностью медицинской помощи, а также для контроля доступности, качества, безопасности, равных условий медицинской помощи и эффективности затрат на нее.

Эта категория цели может возникать при выполнении следующих действий:
- обеспечение управления оказанием медицинской помощи, например планирования ресурсов;
- расследование страхового мошенничества и злоупотреблений при оказании медицинской помощи;
- выполнение функций надзорных органов;
- выполнение экспертиз медицинской помощи и мониторинга сроков ее предоставления и т. д.;
- поддержка или улучшение информационных и сопутствующих систем, служб и программ;
- контроль качества оказанной медицинской помощи;
- контроль организационной и профессиональной аккредитации;
- оценка качества работы медицинских специалистов;
- проведение финансового аудита, оценка рыночного положения и оснащенности ресурсами;
- проведение судебно-медицинской экспертизы медицинской помощи, оказанной ее субъекту;
- проведение внутреннего расследования.

А.7 Обучение

Если студенты во время учебы непосредственно вовлечены в оказание субъекту медицинской помощи, то цель использования ими данных следует характеризовать как оказание медицинской помощи, а не учебу. Данная категория целей не включает ситуацию, когда медицинский работник использует медицинскую информацию о субъекте медицинской помощи для санитарного просвещения субъекта или его представителя. Она подпадает под категорию 1 — оказание медицинской помощи. Если данные используются для «чистого» обучения, то они ни в коем случае не должны быть идентифицируемыми.

Эта категория цели может возникать при выполнении следующих действий:
- непрерывное повышение квалификации и переподготовка;
- обучение студентов;
- представление случая медицинской помощи на врачебной конференции.

А.8 Санитарно-эпидемиологический контроль

Полезность информации, собираемой с этой целью, имеет тенденцию возрастать, если эта информация относится к уменьшающейся популяции. Тем самым оправдано использование идентифицируемых данных.

Эта категория цели может возникать при выполнении следующих действий:
- мониторинг безопасности, например лекарственных средств, инфекционных заболеваний, включая уведомление органов санитарно-эпидемиологического надзора;
- отслеживание контактов при инфекционных заболеваниях;
- предупреждение вспышек инфекционных заболеваний, например карантин, эпидемиологическое расследование;

- выявление субъектов популяции, которым требуется наблюдение врача, например в связи с обнаруженными нарушениями безопасности лекарственных средств или медицинских изделий.

Примечание — Эти действия приносят непосредственную пользу субъекту медицинской помощи и могли бы рассматриваться как относящиеся к категории «оказание медицинской помощи»;

- контроль распространения инфекционных заболеваний, непредвиденных нежелательных явлений, связанных с лекарствами или иммунизацией, регистрация инцидентов, связанных с безопасностью субъектов медицинской помощи, и т. д.;
- надзор за травматизмом;
- мониторинг инфекционных заболеваний санитарно-эпидемиологической службой.

А.9 Экстренные санитарно-эпидемиологические мероприятия

Использование информации с этой целью осуществляется в случаях значительных угроз здоровью или жизни населения, когда необходимы экстренные санитарно-эпидемиологические мероприятия. Эта категория цели может возникать при выполнении следующих действий:
- расследование угроз биотерроризма и борьба с ними;
- проведение масштабных санитарно-эпидемиологических мероприятий при катастрофах, например крушении или наводнении.

А.10 Управление организацией здравоохранения

Здоровье населения изменяется в течение длительного времени и управление им в меньшей степени зависит от здоровья отдельных лиц. Использование информации с этой целью приносит пользу популяции в целом или большой группе населения, поэтому идентифицируемые данные не столь широко используются, хотя и могут требоваться для установления связи данных с другими источниками информации, позволяющей идентифицировать часто повторяющиеся ситуации.

Эта категория цели может возникать при выполнении следующих действий:
- информирование о состоянии общественного здоровья, мероприятиях и политике по его укреплению;
- наблюдение за состоянием общественного здоровья;
- проведение в жизнь обоснованной политики укрепления здоровья;
- эффективное управление системой здравоохранения;
- санитарное просвещение населения, включая информирование о способах поддержания хорошего здоровья.

А.11 Научные исследования

Для обобщающих исследований в зависимости от их характера могут требоваться или не требоваться идентифицируемые данные. Это зависит от политик, юридических и этических норм и характера исследования.

Примечание — В [11] исследование определено как «систематическое изучение в целях установления фактов, принципов или обобщенного знания».

Эта категория цели может возникать при выполнении следующих действий:
- проведение клинических испытаний с согласия пациентов;
- проведение исследований популяции, например: клинических, эпидемиологических, фармацевтических, биоинформационных, биоинженерных, актуарных, включая исследования с помощью интеллектуального анализа данных;
- отбор для клинических испытаний или других исследований;
- контроль научно-исследовательской работы.

А.12 Маркетинговые исследования

Использование информации с этой целью осуществляется при анализе обращения лекарственных средств и деятельности организаций здравоохранения.

Эта категория цели может возникать при выполнении следующих действий:
- проведение маркетинговых и постмаркетинговых исследований и информирование об их результатах.

А.13 Юридическая процедура

Использование информации с этой целью осуществляется при применении законодательства, осуществлении правосудия и исполнении судебных актов.

Примечание — При осуществлении правосудия уполномоченный орган может затребовать раскрытия данных, не указывая явно цель их использования. Однако реальную цель можно установить по журналам доступа и связать ее с органом, затребовавшим раскрытия данных.

Эта категория цели может возникать при выполнении следующих действий:
- использование электронных медицинских карт органами следствия, судебными органами или иными уполномоченными государственными органами;

- использование электронных медицинских карт в уголовных расследованиях и при проведении судебно-медицинской экспертизы;
- защита от угрозы личной безопасности, исходящей от субъекта медицинской помощи, при которой использование его медицинских данных санкционировано или затребовано;
- использование электронных медицинских карт в судебном разбирательстве или планируемом судопроизводстве.

А.14 Использование субъектом медицинской помощи

Субъекту медицинской помощи доступны все категории использования. Однако доступ к своим собственным данным и их использование рассматриваются как неотъемлемые права лица, и когда субъект медицинской помощи или его представитель цели обращаются к данным субъекта, то указание цели использования является необязательным свойством. В некоторых случаях такую цель стоит указывать, даже если такое разъяснение может быть необязательным. В дополнение к другим указанным здесь целям использования субъект медицинской помощи может требовать доступа к своим данным для выполнений следующих действий:

- самостоятельное управление здоровьем и самолечение;
- оздоровление и планирование образа жизни;
- уход на дому, выполняемый членом семьи или другим неформальным участником;
- информирование семьи и заинтересованных третьих сторон об анамнезе жизни;
- получение второго мнения о лечении;
- переход к другому врачу;
- самостоятельное проведение анализа лечения;
- выполнение требований по приему на работу, например предоставление сведений об иммунизации, результатов теста на наркотики, фактов, имевших место в прошлом;
- выполнение иммиграционных или иных требований к выезжающим за границу.

Примечание — Эта категория использования связана с правом субъекта медицинской помощи на раскрытие ему своих медицинских данных, но при этом субъект может указывать или не указывать цель использования данных. Однако реальную цель можно установить по журналам доступа.

А.15 Неуточненная

Эта категория цели может использоваться, если при авторизации доступа не требуется ее указывать или если цель нельзя отнести ни к какой другой категории:

- объявление цели не требуется;
- цель не сообщается;
- другая.

Библиография

[1] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[2] ISO 10181-3, Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework

[3] ISO/TS 13606-1:2008, Health informatics — Electronic health record communication — Part 1: Reference model

[4] ISO/TS 13606-4:2009, Health informatics — Electronic health record communication — Part 4: Security

[5] ISO 18308:2011, Health informatics — Requirements for an electronic health record architecture

[6] ISO/TS 21298, Health informatics — Functional and structural roles

[7] ISO/TS 22600-1:2006, Health informatics — Privilege management and access control — Part 1: Overview and policy management

[8] ISO/TS 25237:2008, Health informatics — Pseudonymization

[9] ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002

[10] ISO/IEC 2382-8:1998, Information technology — Vocabulary — Part 8: Security

[11] Tri-Council Policy Statement, Ethical Conduct for Research Involving Humans, Medical Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada. Available at http://www.von.ca/Research%20Ethics/Tri-council%20Policy%20Statement.pdf

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, электронная передача данных, персональная медицинская информация, классификация целей обработки

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Половой*

Сдано в набор 12.11.2018. Подписано в печать 29.11.2018. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,33. Уч.-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru