КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ МЕДИЦИНСКИХ ДАННЫХ В СИСТЕМЕ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ

РУКОВОДИТЕЛЬ НЦНИТ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОГО КЛИНИЧЕСКОГО ИНСТИТУТА ПЕДИАТРИИ ГБОУ ВПО РНИМУ ИМЕНИ Н.И. ПИРОГОВА МИНЗДРАВА РОССИИ

Борис Аркадьевич Кобринский

Исторически проблема конфиденциальности персональных данных пациентов традиционно решалась в медицине на основе врачебной клятвы, часто именуемой клятвой Гиппократа. С появлением электронных аналогов медицинских документов, и в особенности при переходе к электронному документообороту, произошло отчуждение медицинских записей от их источника. В полный рост эта проблема встала при переходе к электронному здравоохранению (e-health), включающему персоноцентрический подход к медицинским записям пациента, что предполагает интеграцию данных о здоровье каждого человека в специализированных центрах обработки данных (ЦОД) разных уровней. В этом случае появляется возможность доступа к базам данных (БД) информационных медицинских систем (ИМС) в течение жизни пациента не только у лечащего врача и многочисленного медицинского персонала, но и у людей, обеспечивающих техническую поддержку (администраторы баз данных). Исходя из этого, права различных групп пользователей на ознакомление с данными пациентов и их коррекцию, то есть уровни доступа к ИМС, должны быть жестко регламентированы.

Переход к электронным медицинским картам (ЭМК) предполагает в качестве обязательного элемента введение идентификационного номера, позволяющего определить принадлежность данных конкретному лицу. Такой подход должен быть реализован с момента определения беременности и появления записей, касающихся плода. В этом случае ему должен присваиваться временный идентификационный номер, что позволит интегрировать всю информацию о состоянии здоровья будущего ребенка, включая факторы риска. Такой идентификатор может включать Ф.И.О. матери (или отца в случае ее смерти) с дополнением буквой «н» (новорожденный) и указанием порядка его рождения при многоплодной беременности. Для этого должен существовать специальный репозитарий, автоматически формирующий в реальном времени временные идентификаторы, что позволит получать их независимо от места проживания беременных.

Факт передачи временного идентификатора женской консультации (или родильному дому при непосредственном обращении туда беременной/родильницы) должен фиксироваться в репозитарии с указанием административной территории (субъект РФ, автономное образование, район/город) и названия/номера медицинского учреждения, запросившего идентификатор (включая проверку аутентификационных сведений медицинского работника). После получения официального свидетельства о рождении ребенка временный идентификатор заменяется на постоянный. В случае смерти ребенка до получения официального свидетельства о его рождении ЭМК должна храниться с временным идентификатором.

Ввиду распределенного характера медицинских данных пациента в течение жизни (женская консультация, родильный дом, поликлиника, стационар и др.) проблема конфиденциальности состоит в организации санкционированного многоуровневого доступа медицинских работников к БД и отдельным ее разделам, с учетом должностных и функциональных (ролевых) обязанностей, особенно в отношении разрешения на коррекцию информации (помодульное ограничение на просмотр, ввод, коррекцию, удаление, копирование, обработку, печать данных). Полный доступ к данным конкретного больного может быть у лечащего врача, заведующего отделением и непосредственных руководителей

более высокого уровня, которые имеют право на контроль деятельности лечащих врачей, а также в случаях обращения за информацией о пациенте со стороны вышестоящих органов управления здравоохранением и по решению судебных органов. Для врачей лабораторной службы, проводящих диагностические исследования, могут быть введены определенные ограничения на просмотр информации о пациенте. Особый контроль предусматривается в отношении доступа к модулю генеалогических данных, включающему сведения о состоянии здоровья родственников больного, и сведений об определенных профессиональных вредностях. Другими словами, осуществляется управление доступом к данным (санкционированный доступ или ограничение прав доступа), основанное на учете личности субъекта (Ф.И.О.) и группы, в которую субъект входит (должностные/ролевые обязанности, вплоть до ограниченных конкретным временны́м отрезком дежурных врачей, получающих доступ ко всем текущим записям больных стационара, исключая сведения родословной) на период дежурства.

Вопросы защиты медицинских персональных данных с использованием стандартов рассматриваются во многих странах, вступивших на путь электронного здравоохранения, среди которых одним из лидеров является Великобритания. Опыт обеспечения режима информационной безопасности (ИБ) в ИМС разного профиля, обобщенный впервые в 1995 году в британском стандарте BS 7799 «Практические правила управления информационной безопасностью», положен Международной организацией по стандартизации в основу стандарта ISO 17799, принятого в 2000 году. Режим информационной безопасности обеспечивается:

- на административном уровне – политикой безопасности организации, в которой сформулированы цели и способы ее достижения;
- на процедурном уровне – путем разработки и выполнения инструкций по ИБ для персонала, а также мерами физической защиты;
- на программно-техническом уровне – применением апробированных и сертифицированных решений, стандартного набора контрмер: резервного копирования, антивирусной и парольной защиты, межсетевых экранов, шифрования данных и т.д.

В отношении коррекции данных, в отличие от их просмотра, требования еще более строгие, а изменения после завершения сеанса работы с ЭМК пациента исключаются. В противном случае при внесении исправлений в ранее созданный и подписанный текст предшествующие записи должны сохраняться, оставаясь недоступными медицинским работникам подразделений при просмотре ЭМК, то есть реализуется механизм подотчетности, именуемый протоколированием действий или аудитом.

Таким образом, ИБ должна обеспечивать как конфиденциальность – защиту от несанкционированного получения информации, так и целостность – защиту от несанкционированного изменения информации. В настоящее время для этого используется электронная подпись (ЭП). Использование средств ЭП позволяет идентифицировать отправителя (автора) электронного документа и гарантировать неизменность содержания (отсутствие искажений информации в электронном документе, поскольку в случае внесения в него изменений электронная подпись теряет силу).

В медицине конфиденциальность и защита данных в информационных системах традиционно обеспечивается на основе принудительного управления доступом, что предполагает использование меток безопасности: метка субъекта (медицинского работника) описывает его благонадежность, а метка объекта (электронного медицинского документа) – степень закрытости содержащейся в нем анкетной или медицинской информации. Система распознавания пользователей ИМС по их персональным идентификаторам с последующей аутентификацией и авторизацией предполагает проверку прав доступа субъекта к определенным ресурсам, то есть разделам ЭМК. Одним из вариантов безопасности ЭМК может быть раздельное хранение анкетной и медицинской информации на разных серверах. В этом случае конкретная ЭМК доступна только в период работы врача с ней (до прекращения сеанса и подписи конкретной медицинской записи).

Пароль пользователя определяет его привилегии доступа к определенной информации и право на определенные действия. К примеру, система паролей федерального генетического регистра, предложенная автором данной статьи и реализованная в Московском НИИ педиатрии и детской хирургии Минздрава России (ныне Научно-исследовательский клинический институт педиатрии в составе ГБОУ ВПО РНИМУ имени Н.И. Пирогова), в общем виде была представлена следующим образом: 1) право входа в информационную медицинскую систему; 2) определенные права работы с родословной (ввод, корректировка и т.п.); 3) право только на просмотр родословной (исключая определенные диагнозы).

Установкой, конфигурированием сервера, регистрацией пользователей и их групп, а также ролей ведает системный администратор. Подобным образом эта проблема решалась до недавнего времени, часто ее именно так решают и сегодня. Но в настоящее время в здравоохранении начинают опираться на современные правовые решения и технические средства для обеспечения конфиденциальности и защиты данных.

В соответствии с Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» электронное сообщение, подписанное электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью. Применение средств ЭП в соответствии с требованиями Федерального закона от 6 апреля 2011 года №63-ФЗ «Об электронной подписи» является одним из условий организации юридически значимого обмена электронными документами. ЭП – это специфический «цифровой код», интегрированный с содержанием электронного документа, позволяющий идентифицировать его отправителя (автора) и установить отсутствие иска-

жений информации в электронном документе. В этом случае однозначно связываются автор документа, владелец подписи и содержание документа (неизменность содержания или целостность). При этом ЭП обеспечивает неотказуемость и неизменяемость в процессе обмена данными по открытым каналам связи, то есть гарантирует подлинность (неискажаемость) и целостность данных.

Требования к обеспечению безопасности персональной медицинской информации, содержащейся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять их обработку с использованием средств автоматизации, определены Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Реализация закона предполагает ряд аспектов:

1. Обследование с целью оценки соответствия требованиям закона о персональных данных (ПДн):
   – сбор сведений об установленном стандартном и специальном программном обеспечении (формуляры на рабочие станции);
   – разработка модели угроз безопасности ПДн.
2. Проектирование системы защиты ПДн в составе ИМС.

Модель угроз содержит данные об угрозах безопасности обрабатываемых в информационных системах ПДн, вызванных:

– перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
– несанкционированным, в том числе случайным, доступом к ресурсам с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы информационной системы ПДн и обрабатываемых в ней данных с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Примерами мероприятий по технической защите ПДн являются:

– защита на случай физического хищения путем криптования (использование Secret Disk);
– определение несанкционированных подключений к сети (управляемые узлы сети (хабы) и специальное программное обеспечение);
– блокировка подключения внешних носителей информации (DeviceLock);
– контроль неизменяемости системных модулей (Secure Pack);
– создание демилитаризованной зоны сети, обеспечивающей невозможность непосредственного поступления данных из Интернета в локальную вычислительную сеть, содержащую ПДн;
– контроль получения сотрудниками организации бумажных копий электронных носителей конфиденциальной информации (при использовании сетевого варианта Secret Disk).

Наиболее часто применяются системы автоматического шифрования данных, передаваемых через Интернет, – VPN-каналы (ViPNet или Virtual Private Network), обеспечивающие полный контроль входящего и исходящего трафика. Возможно также применение криптошлюза – криптомаршрутизатора.

В России с 1 января 2008 года действует национальный стандарт ГОСТ Р 52636-2006 «Электронная история болезни. Общие положения», описывающий понятие электронной истории болезни и требования к ней. Электронная история болезни (ЭИБ), или электронная медицинская карта, – комплекс медицинских записей, содержащих данные о состоянии пациента и назначаемом ему лечении, обрабатываемых и хранимых электронным способом. Электронная история болезни явилась закономерным результатом развития автоматизации и компьютеризации в медицинских учреждениях и ознаменовала своим появлением переход от традиционной истории болезни к электронной медицинской документации. В данном стандарте сформулированы минимальные требования и прописаны механизмы, в соответствии с которыми каждая медицинская организация должна определить для себя необходимый уровень внутренней безопасности и способы ее реализации.

Для электронных медицинских записей необходимо в первую очередь обеспечить:

– неизменность и достоверность на протяжении всего периода их хранения;
– регламентацию прав доступа и конфиденциальность;
– персонифицируемость (возможность определить автора и происхождение записи в любой момент времени – аналог подписи на традиционном бумажном документе);
– регламент коллективной работы.

Защита сетей от внешнего вторжения обеспечивается системами класса Firewall. Защита данных при объединении удаленных локальных сетей в корпоративную сеть может осуществляться, как описано выше, путем туннелирования с шифрованием, то есть организацией VPN-каналов. Наиболее масштабный реализованный проект – это эксплуатация системы данных о младенческой и перинатальной смертности в Тульской области, где обмен данными происходил между всеми детскими медицинскими учреждениями, областным медицинским информационно-аналитическим центром и Московским НИИ педиатрии и детской хирургии Минздрава России. В этом случае данные шифровались в защищенной сети по месту создания первичных баз данных, в таком виде передавались через Интернет адресату, в его защищенную сеть, а затем в этой сети расшифровывались и поступали к сотрудникам для анализа.

Таким образом, безопасность медицинских данных внутри и вне локальных сетей должна регулироваться следующим порядком:

– аутентификация;
– управление доступом (метка субъекта, метка объекта);
– конфиденциальность данных;

– целостность данных;
– невозможность или ограничение отказа от совершённых действий;
– механизм подотчетности всех действий, влияющих на безопасность;
– защита регистрационной информации от искажений;
– криптозащита информации, передаваемой по открытым линиям связи.

Возможно раздельное хранение собственно персональных данных пациента (анкетные сведения, диагнозы) и различных сведений о состоянии его здоровья. Их объединение осуществляется в этом случае только в момент сеанса записи/просмотра/печати конкретного фрагмента электронной медицинский карты и прерывается сразу после его завершения. Во всех случаях возможность обращения к персональным, в том числе медицинским, данным пациента у других медицинских работников, не имеющих соответствующих прав доступа, отсутствует.

Полноценный переход к электронному здравоохранению в соответствии с российским законодательством принципиально невозможен без комплексного решения вопросов защиты электронных медицинских карт в распределенной сети, если доступ к ним предполагается для всех врачей, участвующих в лечебно-диагностическом процессе, в том числе при оказании помощи в экстренных ситуациях.

Следовательно, информационная безопасность в данной сфере – это: 1) комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей; 2) показатель, отражающий статус защищенности информационной системы или центра обработки медицинских данных. В то же время кибербезопасность (сетевая безопасность) должна предусматривать систему мер для предотвращения внешних атак (хакерских и др.).

Таким образом, сегодня перед здравоохранением стоит задача перехода к защите персональных данных, создаваемых и используемых в электронном виде, на основе современных программно-аппаратных средств.

Для снижения затрат на создание систем защиты персональных данных и оптимизации класса информационных систем ПДн необходимо рассмотреть и по возможности использовать следующие инструменты:

– физическая или логическая сегментация информационных систем по классам обрабатываемой информации, выделение сегментов сети, в которых происходит автоматизированная обработка персональных данных;
– введение в процесс обработки персональных данных процедуры их обезличивания, что можно провести путем нормализации баз данных, после чего защите будет подлежать (согласно требованиям регулирующих документов) лишь справочник, позволяющий выполнить обратное преобразование (однако такой подход не может быть применен ко всем случаям постоянной работы с персональными данными в ряде медицинских организаций);
– разделение персональных данных на блоки, что может быть достигнуто, например, за счет использования таблиц перекрестных ссылок в базах данных;
– деперсонификация или анонимизация/псевдонимизация персональных данных с построением таблиц соответствия обезличенных данных конкретным пациентам, которую можно осуществить в отдельных случаях (статистическая обработка, исследовательская деятельность и др.).