Проблемы информационной безопасности персональных данных в условиях электронной медицины

Масума Мамедова

Институт информационных технологий НАНА

masuma.huseyn@iit.ab.az

***Аннотация*— Исследованы проблемы защиты персональных данных в электронной медицине. Приведены подходы к обеспечению информационной безопасности данных о состоянии здоровья в мировой практике, выделены специфические особенности персональных медицинских данных и показаны потенциальные угрозы конфиденциальности и безопасности медицинской и врачебной тайны в информационных системах. Рассмотрены правовые основы защиты персональных медицинских данных в Азербайджане.**

Ключевые слова— персональные медицинские данные; защита информации; безопасность; конфиденциальность; несанкционированный доступ; врачебная тайна; угрозы.

I. Введение

Информатизация практически всех сфер общественной жизни с каждым годом все интенсивнее проникает в сферу медицины. Новые концептуальные подходы к компьютеризации медицины, выраженные в персоно-центрированном подходе к медицинским записям и создании электронной медицинской карты (ЭМК) пациентов, определили направления модернизации здравоохранения, выраженные в разработке электронных аналогов медицинских документов, появлении возможности отделения медицинских данных от их источника, переходе к электронному документообороту, интеграции данных о состоянии здоровья каждого человека в специализированных центрах обработки информации разного уровня. Уровень развития информационных технологий, определивший возможность реализации ЭМК-инфраструктуры, способствовал расширению: а) доступности медицинских услуг вне зависимости от времени и пространства нахождения зарегистрированной медицинской информации; б) технических возможностей по копированию, повторному использованию и распространению информации; в) доступа к средствам массовых коммуникаций. Однако на фоне указанных положительных изменений современные эффективные средства интеграции и быстрой обработки персональных медицинских данных (ПМД) также успешно используются злоумышленниками, создающими угрозу правам и законным интересам человека. Поэтому задача обеспечения информационной безопасности в условиях э-медицины на сегодняшний день достаточно актуальна.

II. Проблемы обеспечения конфиденциальности и безопасности медицинской информации в мировой практике

Международная практика показывает, что уязвимость конфиденциальности и безопасности ПМД являются основными препятствиями на пути эффективного развития электронной медицины (э-медицины). Так, медицинские учреждения (МУ), имеющие доступ к самой закрытой личной информации о человеке, обязаны гарантировать конфиденциальность и безопасность всей врачебной информации. Любые персональные медицинские данные вне зависимости от носителя информации, будучи конфиденциальной, должна надежно управляться как субъектом данных (пациентами), так и поставщиками профессиональной медицинской услуги (медицинским персоналом). Каждая сторона с правами доступа должна быть уверена, что данные, на которые они опираются, были введены уполномоченными лицами.

Типовая медицинская система (МИС), обеспечивающая создание в МУ единого информационного пространства, автоматизирует и оптимизирует организацию лечебно-диагностических процессов и других сторон жизнедеятельности организации, начиная от документооборота и ресурсного учета до ведения электронной истории болезни, клинических записей о пациенте, интеграции с медицинским оборудованием, осуществляет информационную, интеллектуальную поддержку деятельности всех служб медицинского учреждения, а также поддержку принятия врачебных и управленческих решений. Будучи предназначена для поддержки деятельности медицинского учреждения, МИС отличается от других программных продуктов прежде всего тем, что в ней хранится и обрабатывается персональная и конфиденциальная информация. Юридически медицинские сведения о пациентах относятся к информации, составляющей врачебную тайну, доступ к которой ограничен и регламентируется действующим законодательством. В этой связи в МИС обязательно должен быть реализован ряд мер по обеспечению безопасности как информации, так и информационной системы в целом, в противном случае использование данной МИС неправомерно. Любой пользователь МУ, получающий доступ к МИС, несет полную (моральную, административную и уголовную) ответственность за обеспечение конфиденциальности информации, которую он вносит, использует или передает

другим пользователям. Следовательно, обеспечение безопасности и конфиденциальности данных - одна из ключевых требований к современной МИС и его реализация в информационно-коммуникационных и вычислительных системах является актуальной задачей [1-4]. Конфиденциальность ПМД выражена в том, что МУ, получившие доступ к персональным данным, обязаны не раскрывать и не распространять персональные данные без согласия пациента.

В контексте электронной медицины под безопасностью информации подразумевается состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз, а также защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования и блокирования. Согласно мировой практике, информационная безопасность в системе э-медицины должна обеспечивать 1) конфиденциальность (соблюдение врачебной тайны и защиту персональных данных), т.е. защиту от несанкционированного получения информации, 2) целостность, сводящуюся к защите от несанкционированного изменения информации, 3) доступность [5-7].

Концепция персоноориентированного подхода, являющегося главным трендом модернизации здравоохранения в странах ЕС, США, Канады, Австралии и др., базируется на принципе «чем проще доступ к медицинской информации, тем лучше медицинское обслуживание». Этот принцип предполагает упрощение доступа к ПМД пациента (больного), чтобы он мог оперативно получить квалифицированную медицинскую помощь. При этом режим информационной безопасности в этих странах обеспечивается законодательно регулируемыми стандартами. Так, согласно Европейской директиве о защите данных (EU Data Protection Directive (1995)) в странах–членах ЕС обеспечена гармонизация законодательства на уровне единого европейского пространства, и сегодня многие лечебные учреждения вправе иметь доступ к личным медицинским данным больного [8]. Опыт обеспечения режима информационной безопасности (ИБ) в медицинских информационных системах (МИС) разного профиля Великобритании, 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 г. [9]. Режим информационной безопасности обеспечивается: 1) на организационном (административном и процедурном) уровне – политикой безопасности организации, в которой сформулированы цели и способы ее достижения; 2) на процедурном уровне – путем разработки и выполнения инструкций по ИБ для персонала, а также мерами физической защиты; 3) на техническом (аппаратно-программном) уровне – применением апробированных и сертифицированных решений, стандартного набора контрмер: резервного копирования, антивирусной и парольной защиты, межсетевых экранов, шифрования данных и т.д. Для идентификации отправителя (автора) электронного документа (ЭД) и гарантии неизменности его содержания (отсутствия искажений информации в ЭД) используется электронная подпись (ЭП), которая в случае внесения изменений в электронном документе теряет силу.

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 средствами электронной подписи текст предшествующие записи должны сохраняться, оставаясь недоступными медицинским работникам подразделений при просмотре ЭМК, то есть реализуется механизм подотчетности, именуемый протоколированием действий или аудитом [5-9].

Закон о преемственности и подотчетности медицинского страхования (Health Insurance Portability and Accountability Act - HIPAA) представляет собой федеральный закон США, в котором установлены правила обмена личной медицинской информацией и ее защиты от неразрешенного использования. Информация может быть как на бумаге, так и находиться в электронной медицинской карте [10].

III. Специфические особенности персональных медицинских данных

При разработке системы безопасности ПМД и выборе оптимального режима информационной безопасности МИС наряду с необходимостью учета условий и угроз нарушению определенных характеристик безопасности (конфиденциальность, целостность, доступность) следует принять во внимание также специфику, состав, а также участников обработки ПМД. Анализ литературных источников [11-13] дает возможность выделить следующие специфические особенности ПМД пациента:

1.Персональные медицинские данные (информация) пациента, представляющие собой закрытую личную информацию о последнем, полностью находятся в его распоряжении. Это обусловливает особую форму отношений между пациентами (субъектами данных) и пользователями этой информации, т.е. одновременно необходимо защищать данные и интересы частной жизни субъекта данных, ответственность и интересы профессионалов-медиков, законные интересы исследователей и других третьих лиц.

2.Наличие жесткого временного регламента на работу с медицинскими документами, вызванная необходимостью своевременного оказания медицинской помощи. Ухудшение данного показателя по причине усиления режима конфиденциальности информации в ущерб доступности данных для профессионалов может создать угрозу здоровью, а иногда и жизни больного. Поэтому необходимо обеспечить разумный компромисс между тремя составляющими обеспечения ИБ: конфиденциальностью, целостностью и доступностью данных.

3. ПМД, реализуемые в виде одного логического субъекта, могут быть фрагментированы: а) по анкетным данным, позволяющим однозначно идентифицировать

пациента, б) по типу и характеру медицинских данных (данные о диагнозе, состоянии здоровья, рекомендации и назначения, информация о проведенном лечении, статистические данные и т.п.), в) по местонахождению и автору отдельной медицинской информации (регистратура, УЗИ, лаборатория; врачи разного профиля, медсестра, лаборант и пр.). В этом случае конфиденциальную информацию составляет только объединение всех или многих фрагментов данных, тогда как отдельно, сами по себе, фрагменты медицинских данных тайны не составляют.

IV. Потенциальные угрозы конфиденциальности и безопасности персональных данных в МИС

Согласно [11,14,15] при работе с персональными медицинскими данными могут возникнуть различные угрозы информационной безопасности. Прежде всего, это угрозы конфиденциальности и безопасности информации, которые можно разделить на две категории:

1) Организационные угрозы, которые возникают из-за несанкционированного доступа к данным пациента со стороны: а) инсайдера (работника медучреждения); б) аутсайдера (злоумышленника извне); в) уязвимости информационных систем; при этом нарушитель может осуществить несанкционированный доступ к ресурсам сети по ошибке, случайно или со злым умыслом (хакеры, бывшие сотрудники, пациенты и др.).

2) Технические (системные) угрозы, которые возникают из-за нарушений в цепи потока информации вследствие неправомерного или случайного доступа к базе данных, несанкционированного искажения, уничтожения информации, разрушения физических носителей, сбоев в работе оборудования, возникающих при удалении файлов или поврежденных данных, непредвиденные последствия удаленного резервного копирования, несанкционированная модификация (подделка) данных и т.п.

По состоянию на сегодня [16] наибольшую угрозу конфиденциальности и безопасности информации представляют инсайдеры. Ведь злоумышленником может быть любой сотрудник медицинского учреждения, от рядовой медсестры до руководителя высшего ранга. Поэтому решение задачи защиты информации от несанкционированного воздействия внутренних пользователей невозможно только организационными, или только техническими методами защиты. Лишь комплексное применение как организационных, так технических мер при соответствующей правовой поддержке может обеспечить положительный результат.

Несанкционированный доступ к ПМД пациента может иметь достаточно серьезные моральные и материальные последствия для последнего, затрагивающие 1) неприкосновенность частной жизни, 2) личное здоровье и безопасность, 3) финансовую и коммерческую конфиденциальность, 4) неоправданную дискриминацию со стороны работодателей, страховых компаний, 5) препятствия для политического и карьерного роста и пр. [17].

Международная практика показывает, что самая большая угроза для частной жизни в инфраструктуре электронных медицинских карт связана со вторичным использованием ПМД. Это касается тех случаев, когда информация, раскрываемая для определенной цели, впоследствии без авторизации субъекта данных может использоваться для других целей [14]. Кто же еще заинтересован в информации о состоянии здоровья пациентов и может иметь доступ к ним?

Прежде всего, информация о состоянии здоровья пациентов играет важную роль в проведении научных исследований с целью разработки новых методов лечения различных болезней, сбора статистики, проверки фармакологического воздействия новых лекарственных препаратов, улучшения качества здравоохранения и т.п. Тем не менее, раскрытие информации о состоянии здоровья для исследователей вызывает озабоченность относительно нарушения конфиденциальности. Правила, определенные в нормативно-правовых актах, таких как HIPAA (США), позволяют медицинским организациям раскрывать медицинскую информацию для исследователей только в случае, если они получили на это согласие от пациентов при условии обязательного обезличивания персональных данных или в исключительных случаях, предусмотренных законодательством.

В Регламент доступа к информации о состоянии здоровья включены государственные и частные медицинские учреждения, страховые компании, администраторы, врачи, аптеки, работодатели, учебные заведения, научные учреждения, дата-центры, организации по аккредитации и стандартизации, лаборатории, фармацевтические компании, финансовые агенты и т.п. К другой группе третьих лиц, заинтересованных в получении информации о пациенте, относятся родственники, работники здравоохранения, маркетологи, представители различных общественных Программ содействия, кредитные бюро и правоохранительные органы.

V. Правовая основа защиты персональных данных в Азербайджане

Хотя процессы информатизации медицины в Азербайджане пока находятся в начальной стадии развития, тем не менее правовая основа защиты персональных данных в стране имеется. Принятый в 2010 году Закон Азербайджанской Республики «О персональных данных» обязывает все учреждения выполнять необходимые требования по организации обработки и защиты персональных данных. Естественно, этот закон распространяется и на медицинские учреждения.

В настоящее время информационная безопасность ПМД в Азербайджане регулируется следующими политическими документами:

1. Всеобщая декларация прав человека, принятая ООН 10 декабря 1948 г.

2. Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных», принятая 28 января 1981г. и в 2009 г. ратифицированная Милли Меджлисом Азербайджана (вступила в силу в сентябре 2010 г.).

3. Конституция Азербайджанской Республики, принятая 3 августа 2003г.

4. Закон Азербайджанской Республики «О персональных данных» от 11 мая 1910 г.

5. Закон Азербайджанской Республики об охране здоровья населения, принятый 25 июня 1997 г.

6. Закон Азербайджанской Республики "Об электронной подписи и электронном документе" от 9 марта 2004 г.

7. Закон Азербайджанской Республики "Об информации, информатизации и защите информации" от 3апреля 1998 г.

Целью законодательства Азербайджана в области ИБ персональных данных является обеспечение защиты прав и свобод гражданина при обработке его данных, в том числе защита прав на неприкосновенность частной жизни, личной и семейной тайны. Однако, как показывает мировая практика, интерпретация закона через призму персональных медицинских данных в условиях формирования э-медицины порождает множество споров и разногласий, вызванных спецификой данных о здоровье пациентов. Поэтому во многих странах мира разработаны специфические нормативно-правовые акты, регулирующие информационную безопасность ПМД [8,9,10,18]. С нашей точки зрения, разработка нормативных документов, регламентирующих порядок защиты и обеспечения безопасности сведений, составляющих врачебную и медицинскую тайну, также и в Азербайджане может содействовать усилению защиты неприкосновенности ПМД и акцентировать внимание руководителей медучреждений, медицинского персонала и других заинтересованных сторон к проблеме защиты личной информации пациентов, хранящейся как на бумажных, так и на электронных носителях информации.

VI.ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило сделать следующие заключения:

1. Информационная среда для поддержки как управленческой, так и лечебно-диагностической деятельности МУ является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал. Поэтому обеспечение информационной безопасности ПМД представляет собой комплексную задачу, для решения которой необходимо применение как законодательных, так и организационных и программно-технических мер.

2. Проблема обеспечения защиты персональных данных в учреждениях здравоохранения имеет свою специфику, выраженную в том, что для обеспечения безопасности ПМД в информационных системах медицинских учреждений необходимо выполнение не только требований закона Азербайджанской Республики «О персональных данных», но и комплекса мер по охране врачебной тайны, декларированной Законом Азербайджанской Республики об охране здоровья населения (статья 53).

3. В странах СНГ, в т.ч. и в Азербайджане, взаимоотношения медицинских работников, пациентов и их доверенных лиц/родственников юридически не проработаны. В этой связи целесообразным представляется разработка в республике нормативных документов, регламентирующих порядок защиты и обеспечения безопасности сведений, составляющих врачебную и медицинскую тайну.

БИБЛИОГРАФИЯ

[1] H. Chao, S. Twu, C. Hsu, “A patient-identity security mechanism for electronic medical records during transit and at rest,” II Medical Informatics and the Internet in Medicine, vol.30, no.3, pp. 227-240, 2005.

[2] А. А. Абдуманонов, М. К. Карабаев, “Алгоритмы и технологии обеспечения безопасности информации в медицинской информационной системе Externet,” Программные продукты и системы. №1, стр. 150-155, 2013.

[3] J. Wang, Z. Zhang, X. Yang, L. Zuo, J-U. Kim, “Data security and privacy of e-healthcare in electronic medical environment.” http://onlinepresent.org/proceedings/vol22_2013/17.pdf

[4] W.Wilkowska, M. Ziefle, “Privacy and data security in e-health: Requirements from the user’s perspective,” Aachen University, Communication Science, Germany/Health Informatics Journal, vol. 18, no. 3, pp. 191-201, 2012.

[5] Б. А. Кобринский, “Конфиденциальность и защита персональных медицинских данных в системе электронного здравоохранения.” http://federalbook.ru/files/FSZ/soderghanie/Tom%2015/Kobrinskiy.pdf

[6] M. A. Ameen, J. W. Liu, K. Kwak, “Security and privacy issues in wireless sensor net-works for healthcare applications,” Journal of Medical System, vol. 36, no. 1, pp. , 2012.

[7] D. B. Baker, “Privacy and security in public health: maintaining the delicate balance between personal privacy and population safety,” Computer Security Applications Conference, 2006. http://www.himss.org/files/HIMSSorg/content/files.

[8] European Parliament and Council Directive 95/46/ EC of 24 October 1995. http://europa.eu/legislation_summaries

[9] И. Медведовский, “ISO 17799: Эволюция стандарта в период 2002-2007.” http://dsec.ru/ipm-research-center/article/iso17799

[10] Y. B. Choi, K. E. Capitan, J. S. Krause, M. M. Streeper, “Challenges associated with privacy in healthcare industry: implementation of HIPAA and security rules,” Journal of Medical Systems, vol. 30, no. 1, pp. 57–64, 2006.

[11] Г. И. Назаренко, А.Е.Михеев, П.А.Горбунов, Я.И.Гулиев, И.А.Фохт, О.А. Фохт, “Особенности решения проблем информационной безопасности в медицинских информационных системах. http://www.interin.ru/datas/documents/pib.pdf

[12] R. Agrawal, C. Johnson, “Securing electronic health records without impeding the flow of information,” International Journal of Medical Informatics, vol. 76, no. 5-6, pp. 471-479, 2007.

[13] L. O. Gostin, J. G. Hodge, “Personal privacy and common goods: A framework for balancing under the national health information privacy rule,” Minnesota Law Review, vol. 86, pp. 1439-1449, 2002.

[14] S. Brands. “Privacy and security in electronic health.” http://www.credentica.com/ehealth.pdf

[15] A. Appari, M. E. Johnson. “Information security and privacy in healthcare: current state of research,” 2008. http://www.ists.dartmouth.edu/library/416.pdf.

[16] McAfee Labs Threats Report – February 2015. http://www.mcafee.com/ru/security.

[17] L. B. Harman, C. A. Flite, K. Bond. “Electronic health records: privacy, confidentiality, and security,” AMA Journal of Ethics, vol. 14, no. 9, pp. 712-719, 2012.

[18] J. G. Hodge, L. O. Gostin, P. D. Jacobbson, “Legal Issues Concerning Health Information: Privacy, Quality, and Liability,” Journal of American Medical Association, vol. 282, no. 15, pp, 1466-1471, 1999.