

Особенности
обеспечения защиты
персональных данных
в медицине



«...Надо перейти к ведению истории болезни в электронном виде»

Из вступительного слова Д. А. Медведева
на заседании Совета по развитию
информационного общества в России 12.02.2009 г.

Практически ни одно медицинское учреждение – государственное, муниципальное или частное, не обходится в своей деятельности без использования компьютеров для обработки персональных данных сотрудников и пациентов. Это влечет за собой необходимость организации обработки и защиты персональных данных (ПДн) в соответствии с требованиями действующего законодательства в данной области. Обеспечение безопасности персональных данных в информационных системах медицинских учреждений – это не только выполнение требований Федерального закона «О персональных данных» (№ 152-ФЗ), но и комплекс мероприятий по охране врачебной тайны, понятие которой устанавливается «Основами законодательства Российской Федерации об охране здоровья граждан» (№ 5487-1 от 22 июля 1993 г.).

В большинстве лечебно профилактических учреждений информационные системы создавались без учета требований по защите персональных данных и врачебной тайны, поэтому перед такими учреждениями здравоохранения встает проблема создания соответствующей всем нормативным требованиям интегрированной системы защиты для уже существующих информационных систем, либо перехода к применению новых информационных систем персональных данных (ИСПДн) с реализованными функциями защиты.

В ИСПДн учреждений здравоохранения обрабатываются как персональные данные пациентов, так и ПДн собственных сотрудников.

Правовым основанием для обработки персональных данных сотрудников медицинского учреждения являются Трудовой кодекс (Глава 14) и Постановление Госкомстата РФ от 5 января 2004 г. №1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты» (этот же документ позволяет определить сроки обработки таких ПДн).

Правовым основанием для обработки персональных данных пациентов являются упомянутые выше «Основы...», а так же другие нормативные правовые акты, общие для всей сферы здравоохранения в целом (например, приказы Минздрава «Об утверждении форм первичной медицинской документации учреждений здравоохранения», «Об утверждении учетной и отчетной медицинской документации») или характерные для какой-либо отдельной области медицинского дела (например, Закон Российской Федерации «О донорстве крови и

ее компонентов», приказ Минздрава «Об учреждении форм первичной медицинской документации для учреждения службы крови», приказ Минздрава «Об утверждении порядка медицинского обследования донора крови и ее компонентов», приказ Минздрава «Об учреждении форм первичной медицинской документации для учреждения службы крови» и др.).

Сроки обработки персональных данных в ЛПУ как правило определяются указанными выше приказами Минздрава, а так же приказом «О введении в действие положения о медицинском архиве лечебного учреждения».

При обработке персональных данных пациентов медицинских учреждений следует учитывать, что Федеральный закон «О персональных данных» относит данные о состоянии здоровья пациента к специальной категории ПДн, обработка которых разрешается только при наличии письменного согласия субъекта персональных данных или в исключительных случаях, предусмотренных статьей 10 указанного закона (например, когда обработка ПДн необходима для защиты жизни или здоровья субъекта, либо жизни или здоровья других лиц, и получение согласия субъекта невозможно или когда обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну).

Факт обработки специальной категории ПДн влияет на класс информационной системы (в соответствии с приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» такой ИСПДн присваивается наивысший класс К1), а следовательно и на требования, предъявляемые к системе защиты персональных данных.

Характерной особенностью организации обработки ПДн в ЛПУ является то обстоятельство, что «Основы законодательства РФ об охране здоровья граждан» (статья 31) требуют предусмотреть в ИСПДн медицинских учреждений возможность предоставления пациенту в доступной для него форме информации о состоянии его здоровья, включая сведения о результатах обследования, наличии заболевания, его диагнозе и прогнозе, методах лечения, связанном с ними риске, возможных вариантах медицинского вмешательства, их последствиях и результатах проведенного лечения. Это требование вполне соотносится с положениями и статьи 14 ФЗ «О персональных данных», определяющей право

субъекта персональных данных на доступ к своим персональным данным. Так же следует обеспечить возможность информирования пациентов о способах и сроках обработки и хранения их ПДн, а так же лицах, имеющих к ним доступ.

Для обеспечения безопасности персональных данных пациентов медицинских учреждений необходимы не только технические, но и организационные меры защиты. Особенность обработки персональных данных в медицинских учреждениях заключается так же в том, что передача сведений, составляющих врачебную тайну, разрешена только с согласия пациента, за исключением случаев, предусмотренных статьей 61 «Основ законодательства РФ об охране здоровья граждан». ФЗ-152 несет в себе аналогичные требования (статья 6) и в этом смысле дополняет «Основы...».

Техническая составляющая системы защиты персональных данных в медицинских учреждениях создается в соответствии с требованиями руководящих и методических документов регуляторов. В большинстве случаев состав угроз информационной безопасности требует применения более широкого класса механизмов безопасности, нежели это предусмотрено руководящими и методическими документами (поскольку часто, помимо собственно ПДн, предусматривается защита иных категорий конфиденциальной информации). В таких случаях осуществляется разработка системы защиты ПДн в составе более масштабной комплексной системы обеспечения информационной безопасности, реализующей дополнительные требования по обеспечению защиты информации. Объединение в одном проекте системы защиты персональных данных и комплексной системы обеспечения информационной безопасности позволяет более рационально осуществлять инвестиции в защиту информации.



107023,
Россия, Москва
ул. Семеновская Б., 45
Тел.: +7 (495) 730-74-88
Факс: +7 (495) 580-51-15
info@inforion.ru
www.inforion.ru