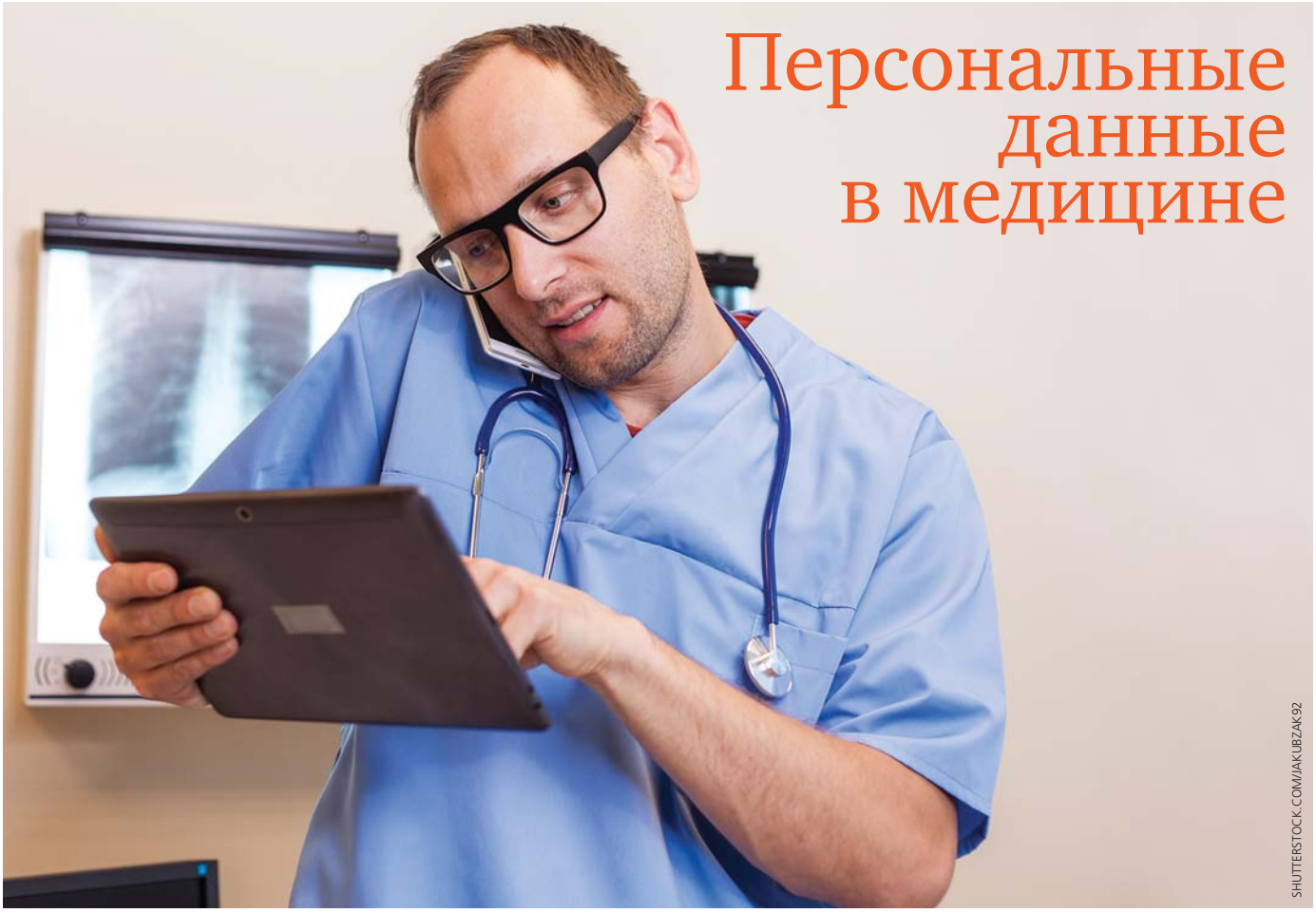
ПЕРСОНАЛЬНЫЕ ДАННЫЕ В МЕДИЦИНЕ
СТР. 33

ТЕМА НОМЕРА

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ



Персональные данные в медицине

SHUTTERSTOCK.COM/JAKUBZAK92

Тема обработки персональных данных обсуждается достаточно давно и, хотя не потеряла своей актуальности, с одной стороны, порядком всем надоела, с другой – в некоторых сферах ситуация с обработкой и защитой персданных остается, **скажем так, сложной**

ВЛАДИМИР ЖУРАВЛЕВ,
заведующий кафедрой юридических проблем защиты конфиденциальной информации Учебного центра «Информзащита»

Тема обработки персональных данных обсуждается достаточно давно и, хотя не потеряла своей актуальности, с одной стороны, порядком всем надоела, с другой – в некоторых сферах ситуация с обработкой и защитой персданных остается, скажем так, сложной.

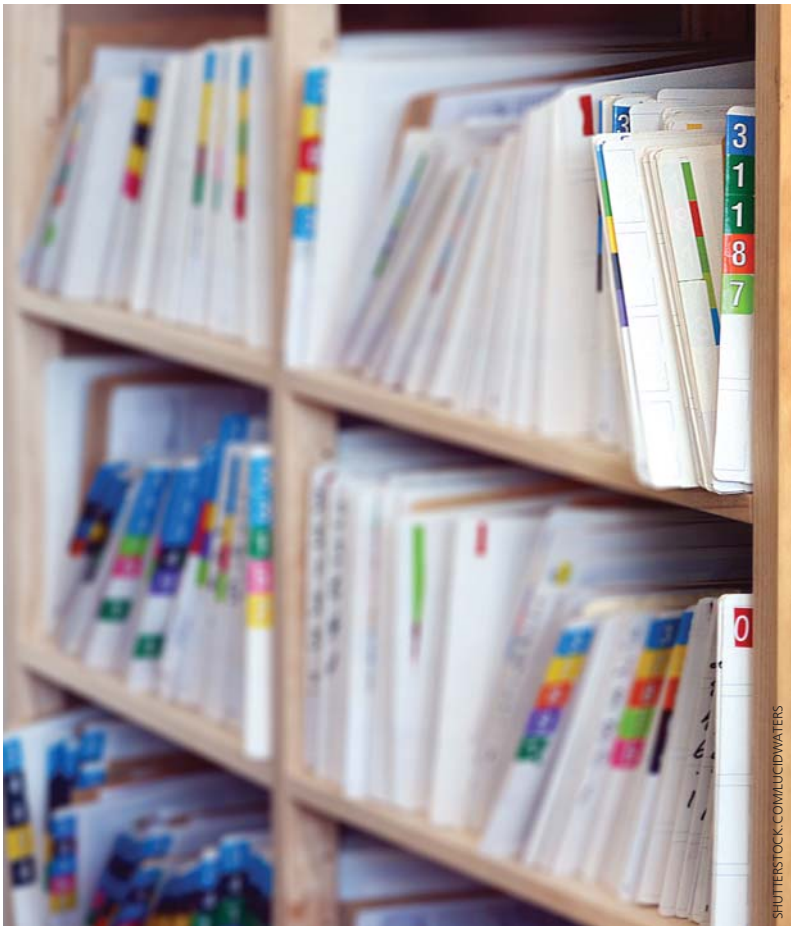
Каждый, кто заходил в поликлинику, лично видел, как хранится «специальная категория персональных данных» – сведения о состоянии здоровья. Конечно, в различных учреждениях ситуация может отличаться, но комната с медицинскими картами – неотъемлемая составляющая почти любой поликлиники. Эта комната – проклятие и спасение для персональных данных.

Проклятие потому, что получить туда доступ зачастую не составляет особого труда. Достаточно, чтобы карта больного не была найдена сразу и отсутствовала у врача. В таком случае больного иногда пускают в хранилище самостоятельно поискать свою карту. Дальнейший контроль над его действиями осуществляется весьма условно.

К сожалению, беды медучреждений на этом не заканчиваются; значительную долю проблем в безопасности создают сотрудники, которые просто не ведают, что творят. Например, в одном из личных блогов пациента сыктывкарской больницы описан случай о повторном использовании больничных бланков, где на обороте была указана дата рождения, номер паспорта, СНИЛС, домашний адрес и иная информация. Становится даже интересно, сколько денег удалось сэкономить таким образом. Спасение состоит в том, что массовые «утечки» в таких случаях практически исключены.

Однако автоматизация пробралась и в медучреждения, особенно это характерно для «дорогих» и солидных заведений. Истории болезни превратились в электронные медицинские карты. Данные в медкартах накапливаются, систематизируются и, соответственно, привлекают злоумышленников. По данным, опубликованным на med-info.ru/content/view/7281, «На черном рынке стоимость медицинских сведений примерно в 10 раз выше цены за финансовую информацию (номера счетов, кредитных карт, проводки и так далее)», и чем выше уровень клиники, тем привлекательней данные о ее клиентах, людях не бедных и старающихся не афишировать свои проблемы и болезни, особенно интимного свойства. Если ЛПУ допускает утечку медицинских сведений, то 48 % пациентов готово это само учреждение поменять. Хотя эта статистика касается США, проблем со сменой клиники не возникнет и у наших соотечественников. А это значит, что медицинское учреждение недополучит денежные средства и т. д. По данным компании InfoWatch (https://www.infowatch.ru/presscenter/news/11245#), в 2014 году зафиксирован очередной рост числа утечек в России на 73 %, и медицинские учреждения набрали целых 25 % от общего числа утечек. Все логично. Привлекательность информации растет, и это манит различных жуликов, а вот защита, особенно в условиях спада финансирования, отстает.

Защита ИСПДн (информационных системах персональных данных), в том числе содержащих сведения о состоянии здоровья, прописана в 1119 постановлении правительства и 21-м приказе ФСТЭК России и ФСБ 378-м приказе ФСБ России. Даже небольшая больница или поликлиника попадает под весьма жесткие требования по 3-му уровню защищенности (УЗ-3), а набрав более 100 000 записей – и под УЗ-2, что предусматривает достаточно обширный набор защитных



SHUTTERSTOCK.COM/LUCIDWATERS

SHUTTERSTOCK.COM/PRESSMASTER

мер. Но отсутствие должного финансирования для закупки и внедрения средств защиты, а также специалистов, которые смогли бы в дальнейшем эффективно эксплуатировать эту систему, не позволяет говорить о появлении надежных систем защиты в данной области.

Еще одна непростая проблема для медицинских учреждений – обеспечение законности обработки персональных данных пациентов. В законе «О персональных данных» предусмотрена отдельная 10-я статья, которая перечисляет случаи, когда можно работать с персональными данными даже без согласия, в том числе в п. 4 говорится, что «обработка персональных данных осуществляется… 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». К сожалению, там прописано весьма неудобное ограничение: все, кто работает со специальной категорией, должны быть профессиональными медиками, иначе необходимо получать письменное согласие либо искать иное основание для обработки. Такое основание действительно существует – это 13 статья в ФЗ № 323 «Об основах охраны здоровья граждан в Российской Федерации», где в пункте 4 предусмотрено десять случаев, когда «врачебную» тайну можно обрабатывать без согласия гражданина. Однако для обычного медучреждения разбираться еще и в юридических тонкостях становится неподъемной задачей. Ведь зачастую тут приходится обойтись вообще без финансирования, т. к. считается, что почитать законы может каждый, читать-то все умеют. Это, в свою очередь, приводит к необоснованным нарушениям прав пациентов и к головной боли для руководителей медучреждений. Приведу лишь два примера.

В законе «О персональных данных» предусмотрена отдельная 10-я статья, которая перечисляет случаи, когда можно работать с персональными данными даже без согласия

SHUTTERSTOCK.COM/DEREK@HATFIELDDESIGN.COM

● До сих пор встречаются случаи, когда от больных требуют письменное согласие на передачу их персональных данных в страховую компанию, хотя еще в 2011 году была предусмотрена возможность такой передачи без согласия (ч. 8 ст. п. 2 ст. 10 ФЗ «О персональных данных»).

● Требование от субъекта согласия – распространенная, но не всегда безопасная затея. Например, в 2012 году Советский районный суд г. Астрахани (дело № 2 -2739/2012) признал требование согласия со стороны ГБУЗ АО «Областной наркологический диспансер» от «гражданки», направленной работодателем на осмотр, незаконным со всем вытекающими последствиями и предписаниями на устранение нарушений.

Подобные случае не являются единичными. РКН на своем сайте постоянно публикует информацию о проведенных проверках и их результатах, мне особо запомнилась проверка еще 2011 года в Департаменте здравоохранение Ивановской области, по результатам которой было получено 14 предписаний на устранение нарушений (http://37.rsoc.ru/news/news31219.htm).

Какие же последствия для организации возможны в связи с невыполнением законодательства? Обычно говорят о штрафах, но на настоящий момент они скорей смешные, чем страшные, – 3–10 тыс. Самыми затратными являются предписания на устранения нарушений, а разовое неисполнение в срок законного предписания грозит уже до 20 тыс. (ч. 1 ст. 19.5 КОАП). Но и это цветочки, одним из самых громких случаев, связанных с персональными данными, была дисквалификация руководителя ТНК БП Роберта Дадли (http://www.kommersant.ru/doc/1011666). Основанием послужило нарушение Трудового законодательства. Да-да, персональные данные работников тоже нуждаются в защите (14-я глава ТК РФ). Надо сказать, что в дальнейшем дисквалификация была обжалована, но руководитель в ТНК БП поменялся.

И в конце о самом интересном. В настоящий момент рассматривается проект «Положения о государственном контроле и надзоре за соответствием обработки персональных данных требованиям законодательства Российской Федерации», согласно которому РКН получает новую возможность – «прекращать или приостанавливать обработку персональных данных». Хотя надо отметить, что эта возможность всегда была предусмотрена п. 4 ч. 3 ст. 23 ФЗ № 152 «О персональных данных», но порядок приостановки до настоящего времени прописан не был, а вот указанное положение (п. 9.8) закрепляет, что это могут делать должностные лица РКН, даже в суд не требуется обращаться.

Учитывая, что разбираться в непрофильных для медучреждений законах и сложных технических требованиях очень тяжело, да и отвлекает от основной работы, было бы здорово, если Министерство здравоохранения вновь разработало пакет типовых документов для медицинских учреждений. Ведь в 2009 году оно уже сделало подобный шаг и даже согласовало документы с ФСТЭК России, что, без преувеличения, сродни трудовому подвигу. К сожалению, за шесть лет указанные документы сильно устарели и нуждаются в серьезной доработке.

Ну а пока свежих шаблонов нет, то каждый сам за себя и сам решает, что делать: разбираться самостоятельно, идти учиться или приглашать стороннюю организацию. Однако за последними тоже нужно приглядывать, а для этого опять же надо разбираться в правовых и технических вопросах. ●