**«Особенности обработки персональных данных учреждениями здравоохранения. Практика взаимодействия с уполномоченным органом субъекта в сфере здравоохранения в вопросах профилактики правонарушений в области персональных данных со стороны подведомственных организаций»**

Добрый день уважаемые коллеги!

Вся наша жизнь от рождения и до «финала» так или иначе, связана с учреждениями здравоохранения. Наверное, нет такого человека, который хотя бы раз не обращался за медицинской помощью. А теперь вспомните, какой объем персональных данных собирается в регистратурах медицинских центров, поликлиник, больниц, частных клиник…. Это колоссальный массив данных, содержащий персональные данные большинства жителей нашей страны, если не всех. При этом помимо основных категорий персональных данных, таких как фамилия, имя, отчество, дата рождения и т.п., происходит сбор специальных категорий персональных данных – состояние здоровья, состояние интимной жизни, а также биометрических персональных данных, которые характеризуют физиологические и биологические особенности человека.

Таким образом, не трудно догадаться, что в учреждениях здравоохранения содержится одна из наиболее объемных и «насыщенных» баз персональных данных. В связи с этим трудно себе представить, какой вред может нанести потеря или утечка информации из неё. Из этого следует, что для предотвращения утечки персональных данных необходимо приложить максимум усилий и возможностей. А так ли это просто?

Процесс становления системы медицинских учреждений в том виде, в котором мы его знаем, зародился очень давно и, как следствие, основная часть баз данных учреждений здравоохранения находится на бумажных носителях. В наше время цифровых технологий происходит оцифровка бумажных носителей, внедряются различные системы, позволяющие уйти от «бумаги» и полностью перейти на электронные информационные системы. Этот переходный период является одной из самых главных проблем защиты персональных данных, а именно: необходимо обеспечить защиту различных информационных систем, что требует значительных материальных и трудовых затрат, повышенного внимания и контроля на всех стадиях обработки персональных данных, а также хорошего знания и понимания законодательства Российской Федерации в области защиты персональных данных.

Понятно, что основную нагрузку по защите персональных данных несет непосредственно каждое учреждение здравоохранения. Но далеко не последняя роль в этом важном деле отводится и уполномоченному органу субъекта в сфере здравоохранения (министерствам, департаментам, управлениям…). Уполномоченный орган субъекта в сфере здравоохранения непосредственно влияет на весь рабочий процесс подведомственных ему учреждений здравоохранения, а также в значительной степени на частные структуры здравоохранения.

Так в чем же может быть оказана помощь Уполномоченным органом субъекта в сфере здравоохранения в вопросах защиты персональных учреждениям здравоохранения на подведомственной ему территории?

Это:

- разработка типовых форм внутренних локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в области защиты персональных данных, устранение последствий таких нарушений (методические рекомендации, инструкции, приказы, регламенты и др.) и внедрение их в учреждениях здравоохранения;

- помощь во внедрении современных средств защиты информационных систем персональных данных и организации обучения персонала по работе с ними;

- проведение совещаний или выделение на своих совещаниях времени для вопросов защиты персональных данных и освещения появления новых новелл в законодательстве РФ (возможно и лучше всего - совместно с ТУ Роскомнадзора).

Конечно, такая дополнительная нагрузка на Уполномоченный орган субъекта в сфере здравоохранения не должна остаться без поддержки, ведь разобраться в тонкостях законодательства РФ не в своей сфере деятельности (в данном случае – сфере защиты персональных данных) далеко не просто. И выходом в данной ситуации может быть взаимодействие с территориальными органами Роскомнадзора. Более того, результат такого взаимодействия становится взаимовыгодным.

Приведу пример, успешного взаимодействия Управления Роскомнадзора по Смоленской области с Департаментом Смоленской области по здравоохранению по вопросу исполнения требования ст. 22 и ст. 25 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» оператором (в нашем случае - учреждения здравоохранения) уведомления о намерении осуществлять обработку персональных данных и информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.

После вступления в силу Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» не все операторы (госорганы, муниципальные органы, юр. и физлица) знали о необходимости предоставления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) уведомления о намерении осуществлять обработку персональных данных. В связи с этим Роскомнадзором было принято решение о направлении информационных писем операторам с разъяснением требований ст. 22 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных».

Данная работа Управления Роскомнадзора по Смоленской области с учреждениями здравоохранения была начата в 2008 году и не смогла единовременно охватить все учреждения, действующие на территории Смоленской области, уведомления поступали в небольших количествах, а также имело место составление протоколов по ст. 19.7 КоАП РФ за непредставление (несвоевременное) представление информации. После консультаций по указанному вопросу с Департаментом Смоленской области по здравоохранению было принято решение о направлении разъяснений непосредственно в Департамент, а доведением информации до учреждений здравоохранения займется он сам.

В результате чего в адрес Управления за довольно небольшой срок поступили Уведомления от практически всех подведомственных Департаменту учреждений здравоохранения, количество не подавших уведомление учреждений исчислялось единицами. В дальнейшем этими организациями также своевременно вносились изменения в ранее поданные уведомления.

Тем не менее, в 2016 году в ходе плановой работы с Реестром операторов, осуществляющих обработку персональных данных, было установлено, что на момент проверки значительное число медицинских учреждений (около 50%) не выполнило должным образом требования ст. 22 Федерального закона «О персональных данных» в части представления необходимых изменений и дополнений в ранее поданное уведомление, в связи с вступлением в силу с 01 сентября 2015 года Федерального закона от 21.07.2014 г. № 242 «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» (необходимо было представить сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации). Данная информация была доведена официальным письмом до Департамента Смоленской области по здравоохранению. Следует отметить быструю и правильную реакцию Департамента, который оперативно довел информацию Управления до подведомственных учреждений и установил ограниченные сроки устранения указанных нарушений (недостатков). В результате в течение двух недель в Управление поступило порядка 40 информационных писем о внесении изменений в Реестр операторов, осуществляющих обработку персональных данных. Данная работа напомнила медицинским учреждениям о необходимости проводить регулярные мероприятия с целью защиты персональных данных граждан, как пациентов, так и работников, позволила актуализировать ранее разработанные в этой области документы. И если судить по количеству консультаций, предоставленных специалистами отдела по защите прав субъектов персональных данных, надзора в сфере связи и информационных технологий операторам данной категории по телефону и при посещении отдела, а также по задаваемым вопросам, можно говорить о неповерхностном подходе медицинских учреждений к данной деятельности, а также о хорошей профилактической работе уполномоченного органа субъекта в сфере здравоохранения.

В связи с появлением и увеличением количества частных медицинских организаций аналогичные профилактические мероприятия проводятся и в отношении этой части медицинских учреждений. В связи с характерной «частной» спецификой данных организаций Управление пришло к выводу о целесообразности направления соответствующих писем в адрес каждой конкретной организации без уполномоченного органа субъекта в сфере здравоохранения, который в данном случае является лицензирующим органом. Однако и при таком подходе в практике Управления отмечается игнорирование запросов Управления, что влечет в дальнейшем привлечение таких организаций к административной ответственности по ст. 19.7 КоАП РФ. На данный момент Управлением Роскомнадзора по Смоленской области совместно с Департаментом Смоленской области по здравоохранению прорабатываются варианты доведения норм ст. 22 Федерального закона «О персональных данных» и до указанных организаций.

В ходе тесной работы Управления Роскомнадзора по Смоленской области с Департаментом Смоленской области по здравоохранению принято решение об участии сотрудников Управления в совещаниях проводимых Департаментом, с выступлениями на темы защиты персональных данных.

В заключении хотелось бы сказать, что хорошо организованное взаимодействие ТУ Роскомнадзора с Уполномоченными органами субъектов в сфере здравоохранения приведет к повышению правовой грамотности сотрудников и, как следствие, к снижению количества нарушений в сфере защиты персональных данных со стороны учреждений здравоохранения!

Спасибо за внимание!