

О рекомендациях по обеспечению информационной безопасности при обмене медицинской персональной информацией

Уважаемые коллеги!

В рамках эксплуатации медицинской информационной системы (МИС), разработанной нашей организацией, и планируемого (либо осуществляемого) обмена медицинской персональной информацией с внешними информационными системами и организациями, обращаем ваше внимание на необходимость соблюдения требований законодательства Российской Федерации в области защиты персональных данных и информации.

Обработка и передача медицинской персональной информации относятся к обработке специальных категорий персональных данных и подлежат регулированию, в том числе, Федеральным законом № 152-ФЗ «О персональных данных», Федеральным законом № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», а также подзаконными нормативными правовыми актами и методическими документами уполномоченных органов.

В целях снижения рисков нарушения требований законодательства и обеспечения надлежащего уровня защиты информации при обмене медицинскими персональными данными, рекомендуем рассмотреть и выполнить комплекс организационных и технических мероприятий по обеспечению информационной безопасности, изложенных в методических рекомендациях по организации защищённого обмена медицинской персональной информацией.

Одновременно сообщаем, что организация-разработчик МИС не является специализированной организацией в области проектирования, внедрения и аттестации систем защиты информации и не осуществляет разработку мероприятий по обеспечению информационной безопасности в понимании требований ФСТЭК России и ФСБ России.

В связи с изложенным рекомендуем обратиться в специализированную организацию, обладающую соответствующей лицензией (лицензиями) и компетенциями, для:

- проведения анализа архитектуры информационных систем;
- разработки модели угроз безопасности информации;
- определения уровня защищённости информационных систем персональных данных;
- подбора и внедрения необходимых организационных и технических мер защиты;
- подготовки и выполнения мероприятий по созданию условий для законного и защищённого обмена медицинской персональной информацией.

Реализация указанных мероприятий позволит обеспечить соответствие процессов обработки и передачи медицинских персональных данных требованиям законодательства Российской Федерации и снизить риски привлечения к ответственности по линии контролирующих органов.

Настоящее сообщение носит рекомендательный характер и направлено в целях информационного сопровождения эксплуатации МИС.