УТВЕРЖДАЮ
Главный врач ГАУЗ
«Стоматологическая
поликлиника №2»

_____ Ф.Х.Султанов

От 14 февраля 2018 года

ПОЛОЖЕНИЕ

по проведению работ по
обеспечению безопасности персональных данных при
обработке в ЕГИС
«Электронное здравоохранение Республики Татарстан»

1.Общое положение

Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ЕГИС «Электронное здравоохранение Республики Татарстан» (далее - Положение) является документом, отражающим организационную и техническую составляющие процесса обеспечения безопасности персональных данных, обрабатываемых в Единой государственной информационной системе «Электронное здравоохранение Республики Татарстан».

Положение устанавливает требования к порядку обработки и обеспечению безопасности персональных данных субъектов при их обработке в ЕГИС ЭЗРТ.

Основной целью проведения работ по обеспечению безопасности персональных данных при их обработке в ЕГИС ЭЗРТ является снижение потерь от угроз, связанных с незнанием или непониманием основных положений организационно-распорядительных документов в области информационной безопасности и правил по защите персональных данных.

Положение разработано в соответствии с Федеральным законом от 27 июня 2006 года №152-ФЗ «О персональных данных», Постановлением

Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области защиты персональных данных. Настоящее Положение вступает в силу с момента подписания приказа об утверждении настоящего Положения руководством Организации.

Настоящее Положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным субъектов, а также при проведении работ по защите персональных данных субъектов.

Все сотрудники должны быть ознакомлены с настоящим Положением под роспись.

2.Получение персональных данных субъектов

При получении персональных данных в информационную систему вводятся сведения об источнике персональных данных и должно быть получено согласие субъекта персональных данных на их обработку.

Персональные данные следует получать у самого субъекта персональных данных. Если персональные данные субъекта возможно получить только у третьей стороны, субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено согласие.

Сотрудники, осуществляющие получение персональных данных субъектов, должны сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение . которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок ,его отзыва.

Операторы получают персональные данные непосредственно у субъекта персональных данных или у третьей стороны.

При получении персональных данных непосредственно у субъектов персональных данных операторы должны обеспечить условия, не допускающие необоснованного раскрытия персональных данных третьим лицам, в том числе:

- не должны произноситься персональные данные вслух при заполнении типовых форм, вводе данных в ЕГИС ЭЗРТ, проверке достоверности

предоставленных субъектом сведений на основании документов, удостоверяющих личность;

- все некорректно заполненные типовые формы должны быть гарантированно уничтожены;
- не должны оставлять заполненные типовые формы на рабочих столах, а также при приеме третьих лиц.

При получении персональных данных операторы должны руководствоваться документами «Режим обработки персональных данных», «Регламент передачи персональных данных третьим лицам», «Регламент выгрузки и передачи персональных данных».

3.Хранение, резервное копирование персональных данных субъектов

Хранение персональных данных осуществляется только в серверном сегменте ЕГИС ЭЗРТ. Подразделение, хранящее персональные данные, обеспечивает их защиту от несанкционированного доступа и копирования согласно настоящему Положению и в соответствии с Постановлением Правительства от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСТЭК от 18 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4.Уничтожение персональных данных субъектов

Персональные данные субъектов подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных необходимо прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с момента поступления указанного отзыва.

Уничтожение персональных данных сопровождается составлением акта уничтожения персональных данных.

5.Обеспечение безопасности персональных данных

Посторонним лицам запрещен доступ в помещения, в которых проходит обработка персональных данных субъектов. Порядок доступа к персональным данным описан в документе «Положение о разграничении доступа к ЕГИС «Электронное здравоохранение Республики Татарстан».

В целях обеспечения физической защиты персональных данных субъектов необходимо учитывать следующее:

- порядок приема, учета и контроля деятельности посетителей;
- организация и контроль пропускного режима;
- технические средства охраны, сигнализация; порядок охраны территории, зданий, помещении, транспортных средств.

Для обеспечения технической зашиты персональных данных субъектов необходима реализация следующих средств защиты:

- применение шифрования данных с применением алгоритма шифрования ГОСТ;
- использование средств анализа защищенности системы;
- применение средств антивирусной защиты;
- применение средств контроля целостности;
- использование криптосредств при передаче информации между средствами обработки персональных данных;
- использование средств резервного копирования;
- использование систем бесперебойного питания;
- документальный запрет акустической обработки персональных данных.

Для исключения возможности реализации угрозы несанкционированного доступа к информации в ЕГИС ЭЗРТ следует принять следующие организационные мероприятия:

- определение порядка доступа к защищаемой информации в ЕГИС ЭЗРТ и техническим средствам ее сбора и обработки;
- разработка и оформление правил пересмотра частной модели угроз;
- определение порядка проведения контрольных мероприятий в .ЕГИС ЭЗРТ;

- разработка порядка пропускного режима на объекты, где осуществляется работа с персональным данным.

Защита персональных данных субъектов на электронных носителях обеспечивается следующими мерами:

- регистрация и поэкземплярный учет используемых электронных носителей персональных данных субъектов.
- обеспечение контроля доступа в помещения, в которых хранятся электронные носители персональным данным;
- учет лиц, допущенных к работе с электронными носителями персональным данным;
- проведение разбирательств и составление заключений по фактам нарушения условий хранения электронных носителей персональным данным субъектов.