УТВЕРЖДАЮ

Главный врач

ГБУЗ РБ КРД № 4 г. Уфа

_____ Камалов Э. М.

«14» января 2015 г.

ПОЛОЖЕНИЕ О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В МЕДИЦИНСКОЙ ИНФОРМАЙИОННОЙ СИСТЕМЕ РЕСПУБЛИКИ БАШКОРТОСТАН

В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ БАШКОРТОСТАН КЛИНИЧЕСКИЙ РОДИЛЬНЫЙ ДОМ № 4 ГОРОДА УФА

(ГБУЗ РБ КРД № 4 Г. УФА)

Общие положения

Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства РФ от 17.11.2007 № 781, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008 № 687, и предназначено для регулирования работ по защите персональных данных и обеспечения функционирования ИСПДн «Медицинская информационная система Республики Башкортостан» в соответствии с требованиями действующего федерального законодательства.

Действие Положения распространяется на ИСПДн «Медицинская информационная система Республики Башкортостан» ГБУЗ РБ КРД № 4 г. Уфа, в которой осуществляется обработка персональных данных как с использованием средств автоматизации, так и без использования таковых.

В настоящем Положении используются следующие термины и понятия:

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Настоящее Положение вступает в силу с момента его утверждения руководителя ГБУЗ РБ КРД № 4 г. Уфа и действует бессрочно до замены его новым Положением.

Все изменения в Положение вносятся приказом руководителя ГБУЗ РБ КРД № 4 г. Уфа.

Категории обрабатываемых персональных данных.

Персональные данные, обрабатываемые в Медицинской информационной системе Республики Башкортостан ГБУЗ РБ КРД № 4 г. Уфа, относятся к сведениям конфиденциального характера.

Состав персональных данных, обрабатываемых в ГБУЗ РБ КРД № 4 г. Уфа, определен в «Перечне защищаемых ресурсов ИСПДн».

Основные условия обработки персональных данных.

Обработка персональных данных осуществляется:

после получения согласия субъекта персональных данных, составленного по форме согласно «Типовой форме письменного согласия субъектов персональных данных на обработку их персональных данных», за исключением случаев, предусмотренных частью 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

после принятия необходимых мер по защите персональных данных.

В ИСПДн приказом руководителя назначается сотрудник, ответственный за защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

Лица, допущенные к обработке персональных данных, под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме согласно приложению А к настоящему Положению.

Запрещается:

обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;

осуществлять ввод персональных данных под диктовку.

Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

Обработка персональных данных в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Оператором осуществляется классификация информационных систем персональных данных в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» в зависимости от категории обрабатываемых данных и их количества.

Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

утвержденных организационно-технических документов о порядке эксплуатации ИСПДн, включающих акт классификации ИСПДн, инструкции пользователя, администратора безопасности и администратора ИСПДн;

настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты и других программных и технических средств в соответствии с требованиями безопасности информации;

охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

Порядок обработки персональных данных без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных (при необходимости получения письменного согласия на их обработку);

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

Электронные носители информации, содержащие персональные данные, учитываются в «Журнале учета съемных носителей персональных данных».

При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Бумажные носители персональных данных уничтожаются в присутствии членов постоянно действующей экспертной комиссии с оформлением «Акта об уничтожении персональных данных» по следующей процедуре:

включение каждого отобранного к уничтожению документа (дела) отдельной позицией в акт;

оформление в акте итоговой записи с указанием количества уничтожаемых документов (дел);

письменное согласование акта с руководителями структурных подразделений ГБУЗ РБ КРД № 4 г. Уфа, направивших запрос на уничтожение бумажных носителей;

подписание акта членами постоянно действующей экспертной комиссии.

Перед непосредственным уничтожением бумажных носителей персональных данных членами постоянно действующей экспертной комиссии должна быть осуществлена сверка носителей с описью, приведенной в акте уничтожения.

Бумажные носители персональных данных уничтожаются в присутствии членов постоянно действующей экспертной комиссии в составе не менее 3 человек, принимавших участие в сверке (проверке) документов и дел, подлежащих уничтожению. После уничтожения документов члены постоянно действующей экспертной комиссии производят запись в акте об уничтожении, заверяют ее своими подписями.

Уничтожение документов производится путем сожжения, дробления, растворения или химического разложения, превращения в бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в кусочки площадью не более 2,5 кв. мм.

Доступ к персональным данным

Доступ сотрудников к персональным данным субъектов персональных данных

Сотрудники ГБУЗ РБ КРД № 4 г. Уфа получают доступ к персональным данным субъектов персональных данных исключительно в объеме, необходимом для выполнения своих должностных обязанностей.

Список сотрудников ГБУЗ РБ КРД № 4 г. Уфа, имеющих доступ к персональным данным субъектов персональных данных, приведен в «Положении о разграничении прав доступа к обрабатываемым персональным данным ИСПДн».

Перечень подразделений и сотрудников, допущенных к работе с персональными данными, обрабатываемыми в ГБУЗ РБ КРД № 4 г. Уфа, разрабатывается и пересматривается по мере необходимости (изменение организационно-штатной структуры, введение новых должностей и т. п.) на основании заявок начальников структурных подразделений.

Сотруднику ГБУЗ РБ КРД № 4 г. Уфа, должность которого не включена в перечень подразделений и сотрудников, допущенных к работе с персональными данными, но которому необходим разовый или временный доступ к персональным данным субъектов персональных данных в связи с исполнением должностных обязанностей, приказом руководителя ГБУЗ РБ КРД № 4 г. Уфа может быть предоставлен такой доступ на основании письменного мотивированного запроса непосредственного руководителя сотрудника.

Сотрудник ГБУЗ РБ КРД № 4 г. Уфа получает доступ к персональным данным субъектов персональных данных после:

ознакомления и изучения требований настоящего Положения и иных внутренних нормативных документов по защите персональных данных в части, его касающейся;

прохождения инструктажа о соблюдении правил обработки персональных данных;

ознакомления с видами ответственности за нарушение (невыполнение) норм законодательства РФ в сфере обработки персональных данных.

Доступ субъектов персональных данных к персональным данным

В процессе основной деятельности ИСПДн непрерывно взаимодействует с субъектами персональных данных, требуя от субъекта поддержания своих персональных данных в актуальном состоянии.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных в Медицинской информационной системе Республики Башкортостан ГБУЗ РБ КРД № 4 г. Уфа. Данные сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором, либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Право субъекта персональных данных на доступ к своим персональным данным может быть ограничено в случае нарушения при таковом доступе конституционных прав и свобод других субъектов персональных данных.

Право на получение информации, касающейся обработки персональных данных, действует на протяжении всего срока обработки персональных данных (включая хранение), предусмотренного действующим законодательством Российской Федерации. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными работодатель вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

В случае нарушения установленного федеральным законодательством порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) предусмотрены административные штрафы.

Приложение А

ОБЯЗАТЕЛЬСТВО

о неразглашении информации, содержащей персональные данные

Я,_____,

(Ф.И.О. сотрудника) исполняющий (ая) должностные обязанности по замещаемой должности

_____,

(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ _____

(фамилия, инициалы) (подпись)

«_____»_____ ____г.