Приложение
к приказу ГБУЗ РБ СПБ
№ 108-Д от «08» 01 2024

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
государственного бюджетного учреждения здравоохранения
Республики Башкортостан Стерлитамакская психиатрическая больница
(ГБУЗ РБ СПБ)

г.Стерлитамак

1. Введение

Настоящая Политика определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных в ГБУЗ РБ СПБ с целью защиты прав и свобод человека, и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Политика обработки персональных данных (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 15-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Действие настоящей Политики распространяется на все персональные данные субъектов, обрабатываемые ГБУЗ РБ СПБ с применением средств автоматизации и без применения таких средств.

К настоящей Политике имеет доступ любой субъект персональных данных, Политика публикуется на официальном сайте ГБУЗ РБ СПБ.

Настоящая Политика утверждается главным врачом ГБУЗ РБ СПБ, вступает в силу с момента ее утверждения и действует бессрочно, до замены ее новой Политикой.

Действие настоящей Политики не распространяется на персональные данные, отнесенные в установленном порядке к сведениям, составляющим государственную тайну, порядок обработки которых регламентируется нормативными и методическими документами в области защиты государственной тайны.

1. Правовые основания обработки персональных данных

К правовым основаниям обработки персональных данных относятся:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
- Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

– Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

– Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

– Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

– Устав ГБУЗ РБ СПБ;

– другие действующие нормативно-правовые акты Российской Федерации, Министерства здравоохранения РФ, а также в соответствии с приказами и распоряжениями Министерства здравоохранения Республики Башкортостан, относящиеся к вопросу обработки и защиты персональных данных.

2. Основные понятия

В настоящей Политике используются следующие термины и определения:

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному 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.

Оператор персональных данных — ГБУЗ РБ СПБ, организующий и осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные (далее ПДн) — любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая Учреждению в связи с трудовыми отношениями и ведением деятельности.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Область действия

Положения Политики распространяются на все отношения, связанные с обработкой персональных данных, осуществляемой ГБУЗ РБ СПБ:

– с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с

персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;

– без использования средств автоматизации.

Политика применяется ко всем работникам ГБУЗ РБ СПБ.

4. Порядок и условия обработки персональных данных

ГБУЗ РБ СПБ получает все обрабатываемые им ПДн непосредственно у субъектов ПДн. В случаях, когда получение ПДн непосредственно у субъектов ПДн невозможно, ГБУЗ РБ СПБ предпринимает предусмотренные действующим законодательством меры по соблюдению прав субъектов ПДн при получении их ПДн от третьих лиц.

В случаях, когда действующим законодательством требуется получение согласия субъекта ПДн на обработку его ПДн, ГБУЗ РБ СПБ обрабатывает его ПДн только при наличии такого согласия и с соблюдением ограничений на объем, сроки и способы обработки ПДн, предусмотренных таким согласием.

ГБУЗ РБ СПБ не получает и не обрабатывает ПДн субъекта ПДн о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности.

ГБУЗ РБ СПБ предоставляет своим работникам доступ к минимальному объему ПДн, необходимому им для выполнения своих служебных обязанностей.

Работники ГБУЗ РБ СПБ допускаются к обработке ПДн только после ознакомления с требованиями действующего законодательства и внутренних нормативных и распорядительных документов ГБУЗ РБ СПБ, регулирующих обработку и защиту ПДн, и подписания обязательства о неразглашении конфиденциальной информации.

Персональные данные субъектов ПДн ГБУЗ РБ СПБ должны храниться на бумажных и электронных носителях с ограниченным доступом, в специально предназначенных для этого помещениях в металлических хранилищах. Места хранения материальных носителей персональных данных определяются соответствующими приказами по ГБУЗ РБ СПБ.

В процессе хранения персональных данных ГБУЗ РБ СПБ должны обеспечивать:

– требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

– сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящей Политике;

– контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

Ответственное лицо за обеспечение безопасности персональных данных осуществляет контроль за хранением персональных данных в соответствии с требованиями к учету и хранению конфиденциальных сведений в информационной системе.

Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением правительства РФ 15 сентября 2008 г. №687.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не установлено действующим законодательством. В результате уничтожения персональных данных становится невозможным восстановить содержание персональных данных в информационной системе персональных данных. Материальные носители персональных данных уничтожаются. Решение об уничтожении принимается главным врачом ГБУЗ РБ СПБ, на основании ходатайства ответственного за организацию обработки ПДн.

Уничтожение бумажных носителей должно осуществляться сотрудниками, допущенными к обработке персональных данных, путем, не допускающим дальнейшую возможность ознакомления с данными документами. Уничтожение информации на автоматизированных рабочих местах должно осуществляется комиссией, способами, не позволяющие осуществить восстановление данных.

При уничтожении данных составляется, в обязательном порядке, акт с указанием, какие именно документы и файлы были уничтожены.

5. Передача персональных данных

При передаче персональных данных третьим лицам должны соблюдаться следующие требования:

– не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральными законами;

– предупреждать лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данная Политика не

распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;

– передавать персональные данные субъекта представителям соответствующих государственных органов в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

6. Доступ к персональным данным

Перечень лиц, имеющих право доступа к персональным данным, определяется документом «Перечень сотрудников, осуществляющих обработку персональных данных», утвержденным главным врачом ГБУЗ РБ СПБ. Все лица, допущенные к работе с персональными данными, подписывают обязательство о неразглашении персональных данных субъектов ПДн.

Субъекты ПДн, чьи персональные данные обрабатываются в ГБУЗ РБ СПБ, имеют право:

– получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта, за исключением случаев, предусмотренных Федеральными законами;

– требовать уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для ГБУЗ РБ СПБ персональных данных;

– получать от ГБУЗ РБ СПБ сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– получать от ГБУЗ РБ СПБ сведения о сроках обработки персональных данных, в том числе о сроках их хранения;

– получать от ГБУЗ РБ СПБ сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его персональных данных;

– обжаловать в суде любые неправомерные действия или бездействия руководства ГБУЗ РБ СПБ при обработке и защите его персональных данных.

Передача информации третьим лицам возможна только при письменном согласии субъектов.

7. Обеспечение безопасности персональных данных

Организация работ по обеспечению безопасности персональных данных осуществляется руководством ГБУЗ РБ СПБ.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Учреждения, приказом главного врача ГБУЗ РБ СПБ назначается лицо, ответственное за организацию обработки персональных данных.

Лицо, ответственное за организацию обработки персональных данных, в своей деятельности руководствуется нормативными документами в области обработки персональных данных.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных может осуществляться также сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

Лица, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании утвержденного списка.

Мероприятия по защите персональных данных осуществляются в соответствии с внутренним планом.

Мероприятия по обеспечению безопасности персональных данных при автоматизированной обработке:

Система защиты персональных данных

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

При обработке персональных данных в информационных системах ГБУЗ РБ СПБ должно быть обеспечено:

– Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– Своевременное обнаружение фактов несанкционированного доступа к персональным данным;

– Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– Возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– Постоянный контроль над обеспечением уровня защищенности персональных данных.

Перечень мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

– Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

– Разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

– Проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– Учет лиц, допущенных к работе с персональными данными в информационной системе;

– Контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– Описание системы защиты персональных данных.

Определение уровня защищенности информационных систем персональных данных

Информационные системы персональных данных ГБУЗ РБ СПБ подлежат обязательному определению уровня защищенности.

Для проведения определения уровня защищенности информационных систем, персональных данных Учреждения приказом главного врача ГБУЗ РБ СПБ назначается комиссия.

Результаты определения уровня защищенности оформляются соответствующим актом.

Помещения, в которых ведется обработка персональных данных

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными,

организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Лица, осуществляющие обработку персональных данных в автоматизированном виде обязаны соблюдать требования «Инструкции пользователя информационной системы персональных данных» ГБУЗ РБ СПБ.

Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации:

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Учреждения или лица, осуществляющие такую обработку по договору с Организациям), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

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

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о

цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Организации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;

в) 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;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный 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:

а) 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;

б) 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.

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).

Правила, предусмотренные вышеуказанными пунктами настоящей Политики, применяются также в случае, если необходимо обеспечить

раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

8. Ответственность за разглашение информации, связанной с персональными данными

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, установленных действующим законодательством Российской Федерации и настоящей Политикой, несут дисциплинарную, административную, гражданско-правовую, уголовную и иную ответственность, предусмотренную законодательством Российской Федерации.