Приложение 1

к Приказу № 86

от «30» 06 2021 г.

УТВЕРЖДАЮ

Главный врач А.М. Косов

«____» _____ 2021 г.

ПОЛИТИКА

обработки и защиты персональных данных государственного бюджетного учреждения здравоохранения «Областная клиническая специализированная психоневрологическая больница №1»

Челябинск
2021

СОДЕРЖАНИЕ

1. Основные термины и определения 4
2. Общие положения 5
3. Правовые основания обработки персональных данных 5
4. Цели обработки персональных данных 5
5. Категории обрабатываемых персональных данных 6
6. Принципы обработки персональных данных 6
7. Передача персональных данных 7
8. Меры по обеспечению безопасности персональных данных 7
9. Условия обработки персональных данных 8
10. Ответственность 10
11. Заключительные положения 10

1. Основные термины и определения

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

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

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

Инцидент информационной безопасности – событие, в результате наступления которого произошло разглашение конфиденциальной информации, нарушение работоспособности ИСПДн, внесение несанкционированных изменений, утечка или разглашение персональных данных клиентов и прочих событий, ведущих к нарушению прав и свобод граждан Российской Федерации.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных или наличия иного законного основания.

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 – 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.

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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.

2. Общие положения

2.1. Настоящая Политика обработки и защиты персональных данных (далее – Политика) государственного бюджетного учреждения здравоохранения «Областная клиническая специализированная психоневрологическая больница №1» (ГБУЗ «ОКСПНБ №1», далее – Оператор) является официальным документом, в котором определены общие принципы, условия, цели и порядок обработки персональных данных, а также содержит сведения о реализуемых требованиях к защите персональных данных.

2.2. Политика разработана на основании Конституции Российской Федерации; «Трудового кодекса Российской Федерации» от 30.12.2001 № 197-ФЗ; Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»); Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации 01.11.2012 № 1119; других нормативно-правовых актов в области защиты персональных данных.

2.3. Настоящей Политикой определяется порядок работы с персональными данными субъектов, обратившихся в ГБУЗ «ОКСПНБ №1» или направленными из других медицинский организаций по Челябинской области, и персональными данными работников ГБУЗ «ОКСПНБ №1».

2.4. Целью настоящей Политики является защита интересов ГБУЗ «ОКСПНБ №1», ее пациентов, работников, а также выполнение законодательства Российской Федерации в области защиты персональных данных.

2.5. Настоящая Политика распространяется на всех сотрудников оператора, включая сотрудников, работающих по договору подряда, а также на сотрудников сторонних организаций, взаимодействующих с оператором на основании соответствующих нормативных, правовых и организационно-распорядительных документов.

Настоящая Политика вступает в силу с момента ее утверждения и действует бессрочно, до замены ее новой политикой.

3. Правовые основания обработки персональных данных

3.1. Правовые основания обработки персональных данных пациентов: Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

3.2. Правовые основания обработки персональных данных работников: Трудовой кодекс Российской Федерации от 30 декабря 2001 № 197-ФЗ; постановление правительства Российской Федерации «Об утверждении положения о воинском учете» от 27 ноября 2006 № 719; «Налоговый кодекс Российской Федерации» от 31 июля 1998 г. № 146-ФЗ; Федеральный закон от 01 апреля 1996 г. №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»; приказ Министерства здравоохранения Челябинской области от 25 октября 2018 г. № 2259 «Об использовании прикладного сервиса «Регистр медицинских работников» подсистемы регионального сегмента единой государственной системы в сфере здравоохранения Челябинской области».

4. Цели обработки персональных данных

Оператор обрабатывает персональные данные исключительно в следующих целях:

4.1. Персонала:

– исполнение требований Трудового кодекса РФ;

– исполнение требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога;

– исполнение требований пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение;

– заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством;

– автоматизация процессов получения, переработки, хранения служебной информации.

4.2. Пациента:

– оказание медицинских и медико-социальных услуг.

4.3. Оператор прекращает обработку персональных данных в следующих случаях:

– при передаче персональных данных в архив (хранение документов в архиве организовано в соответствии с Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»);

– при окончании срока хранения и обработки персональных данных;

– при утрате правовых оснований;

– при прекращении деятельности оператора.

5. Категории обрабатываемых персональных данных

5.1. Обрабатываются иные категории персональных данных работников, состоящих в трудовых отношениях с оператором.

5.2. Обрабатываются специальные категории персональных данных пациентов ГБУЗ «ОКСПНБ №1» и иные категории персональных данных их законных представителей.

6. Принципы обработки персональных данных

Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона «О персональных данных». Обработка персональных данных осуществляется на основе следующих принципов:

6.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

6.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

6.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

6.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

6.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

6.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7. Передача персональных данных

7.1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки персональных данных, оператор в ходе своей деятельности предоставляет персональные данные согласно основаниям обработки персональных данных. Передача персональных данных работников осуществляется в Пенсионный фонд РФ, Федеральную налоговую службу, банковские организации, военные комиссариаты, АИС бухгалтерского и кадрового учета учреждений здравоохранения Челябинской области, сервис «Регистр медицинских работников», образовательные организации.

7.2. Передача в электронном виде осуществляется с использованием средств криптографической защиты информации, сертифицированных ФСБ России.

7.3. Передача персональных данных по запросу полиции осуществляется согласно п. 4, ч. 1, ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции».

8. Меры по обеспечению безопасности персональных данных

8.1. Безопасность персональных данных, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных.

8.2. Оператор предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

8.3. Оператор предпринимает следующие организационно-технические меры:

– назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;

– ограничение и регламентация состава работников, имеющих доступ к персональным данным;

– ознакомление работников с требованиями федерального законодательства и нормативных документов по обработке и защите персональных данных;

– обеспечение учёта и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение;

– определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;

– разработка на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;

– проверка готовности и эффективности использования средств защиты информации;

– реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;

– регистрация и учёт действий пользователей информационных систем персональных данных;

– парольная защита доступа пользователей к информационной системе персональных данных;

– применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;

– применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;

– осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;

– применение в необходимых случаях средств межсетевого экранирования;

– применение в необходимых случаях средств обнаружения вторжений в корпоративную сеть, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

– централизованное управление системой защиты персональных данных;

– резервное копирование информации;

– обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;

– учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

– проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;

– размещение технических средств обработки персональных данных, в пределах охраняемой территории;

– поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности.

9. Условия обработки персональных данных

9.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных». Обработка персональных данных допускается в следующих случаях:

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

– обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

– обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средств массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных.

9.2. Обработка оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается в случаях, если:

– субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

– персональные данные сделаны общедоступными субъектом персональных данных;

– обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

– обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, и в связи с осуществлением правосудия;

– обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о противодействии терроризму, о противодействии коррупции, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

– обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка, если иное не установлено федеральным законом.

9.3. В целях информационного обеспечения в ГБУЗ «ОКСПНБ №1» могут создаваться общедоступные источники персональных данных работников, в том числе справочники и адресные книги. В общедоступные источники персональных данных с согласия работника могут включаться его фамилия, имя, отчество, должность, номера контактных телефонов, адрес фактического места жительства и адрес электронной почты.

9.4. Сведения о работнике должны быть в любое время исключены из общедоступных источников персональных данных по требованию работника, либо по решению суда или иных уполномоченных государственных органов.

9.5. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные федеральным законом.

9.6. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

9.7. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

9.8. 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.

9.9. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального законодательства;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством;

- информацию о трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных.

9.10. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

9.11. Сведения, указанные в пункте 9.9 настоящей Политики, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

9.12. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

10. Ответственность

10.1. Ответственный за организацию обработки персональных данных в МАУЗ ГБУЗ «ОКСПНБ №1» назначается приказом главного врача.

10.2. Ответственный за обеспечение безопасности персональных данных в информационных системах ГБУЗ «ОКСПНБ №1» назначается приказом главного врача.

10.3. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

11. Заключительные положения

11.1. Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных.

11.2. Иные права и обязанности оператора персональных данных, определяются законодательством Российской Федерации в области персональных данных.

11.3. Должностные лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

11.4. ГБУЗ «ОКСПНБ №1» имеет право вносить изменения в настоящую Политику.

11.5. Новая редакция Политики вступает в силу с момента ее утверждения и размещения на сайте ГБУЗ «ОКСПНБ №1», если иное не предусмотрено новой редакцией Политики.

11.6. Настоящая Политика обязательна для соблюдения и ознакомления всеми сотрудниками ГБУЗ «ОКСПНБ №1».