

Политика информационной безопасности ОБУЗ «ОКПБ «Богородское»

1. Общие положения

1.1. Настоящая Политика информационной безопасности ОБУЗ «ОКПБ «Богородское» (далее – Политика) разработана в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом ОБУЗ «ОКПБ «Богородское» (далее – Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в Организации осуществляется в связи с выполнением Оператором функций, предусмотренных ее учредительными документами, и определяемых:

- Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Законом РФ от 02 июля 1992 г. N 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении

требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящую Политику.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу Ивановская область, Ивановский р-н, с. Богородское, ул. Б. Клинецовская, д. 2 а, электронная версия Политики – на сайте по адресу: <http://psbbogorod.ru/> .

2. Термины и принятые сокращения

Персональные данные (ПДн) – 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;

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;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

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;

Обезличивание персональных данных – действия, в результате которых становится

невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

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

Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях;

Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

– законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

– системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

– комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;

– непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении

ремонтных и регламентных работ;

- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.

3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

4. Обработка персональных данных

4.1. Получение ПДн

4.1.1. Все ПДн следует получать от самого субъекта или его законного представителя.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПДн создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б) внесения сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

4.2. Обработка ПДн

4.2.1. Обработка персональных данных осуществляется:

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

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

– в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

4.2.2 Цели обработки ПДн:

– обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральным законом от 21 ноября 2011г № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», Законом РФ от 02 июля 1992 г. N 3185-1 «О психиатрической помощи и

гарантиях прав граждан при ее оказании», Федеральным законом от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006, иным законодательством РФ;

- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющие близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью, для решения других вопросов в соответствии с Уставными целями Оператора.

4.2.4. ПДн, обрабатываемые Организацией:

- данные полученные при осуществлении трудовых отношений;
- данные полученные для осуществления отбора кандидатов на работу в организацию;
- данные полученные при осуществлении гражданско-правовых отношений;
- данные полученные при оказании медицинской помощи и иных услуг.

Полный список ПДн представлен в Перечне ПДн, утвержденном главным врачом Организации.

4.2.5. Обработка персональных данных ведется:

- с использованием средств автоматизации.
- без использования средств автоматизации.

4.3. Хранение ПДн

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

4.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не

дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение ПДн

4.4.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

4.5. Передача ПДн

4.5.1. Организация передает ПДн третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

5. Перечень мер по обеспечению безопасности персональных данных при их обработке

5.1. Организация при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

- Назначением лица, ответственного за организацию обработки персональных данных и других лиц, ответственных за обеспечение бесперебойной работы информационных систем, за обеспечение безопасности персональных данных, обрабатываемых в информационных системах, за использование средств защиты информации.
- Утверждением руководителем Организации локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.
- Осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных.

- Ознакомлением работников Организации, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных работников.
- Выполнением требований, установленных постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных, осуществляемой без использования средств автоматизации.
- Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.
- Учетом машинных носителей персональных данных.
- Выявлением фактов несанкционированного доступа к персональным данным и принятием мер.
- Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых в информационных системах персональных данных.
- Наличием у Организации соглашений об обмене информацией со сторонними организациями.

5.2. Работники Организации, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

6. Основные права субъекта ПДн и обязанности Организации

6.1. Основные права субъекта ПДн

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

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн 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.

6.2. Обязанности Организации

Организация обязана:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;
- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн. уполномоченного органа по защите прав субъектов ПДн.