Согласовано
Председатель ПК ГАУЗ «Республиканский наркологический диспансер» МЗ РБ

_____ Я.С. Громакина

«18» 07 2017 г.

Утверждено
И.о.главного врача ГАУЗ «Республиканский наркологический диспансер» МЗ РБ

_____ С.Д. Дамдинов

«18» 07 2017 г.

Политика обработки и защиты персональных данных медицинской организации ГАУЗ «Республиканский наркологический диспансер» МЗ РБ

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п.2 ст.18.1 Федерального закона №152-ФЗ от 27.07.2016 г. «О персональных данных» и является основополагающим внутренним регулятивным документов медицинской организации ГАУЗ «Республиканский наркологический диспансер» МЗ РБ (далее – Организация или Оператор),определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПД), оператором которой является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД 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 ПД, 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 ПД, полученных до ее утверждения.

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

1.4.1. Федеральным законом от 21.11.2011 г. №323 «Об основах охраны здоровья граждан в Российской Федерации»;

1.4.2. Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»;

1.4.3. Постановлением правительства Российской Федерации от 15.09.2008 №687 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.4.4. Постановлением правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.4.5. Иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПД в Организации осуществляется в ходе трудовых и иных, непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя, в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу: 670033, Республика Бурятия, г.Улан-Удэ, ул.Краснофлотская, 44, электронная версия Политики – на сайте по адресу: rndbur.ru

2. Термины и принятые сокращения

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

2.2. 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.

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

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

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

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

2.7. 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.

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

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

2.10. Информационная система персональных данных (ИСПД) – совокупность содержащихся в базе данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.11. Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у

него заболевания и от его состояния. Пациентом может быть как взрослый, так и ребенок.

2.12. 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.

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

3.2. Для обеспечения безопасности ПД Организация руководствуется следующими принципами:

3.2.1. Законность: защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;

3.2.2. Системность: обработка ПД в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД;

3.2.3. Комплексность: зашита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;

3.2.4. Непрерывность: защита ПД осуществляется на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе при проведении ремонтных и регламентных работ;

3.2.5. Своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;

3.2.6. Преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляется на основании результатов анализа практики обработки ПД в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;

3.2.7. Персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПД;

3.2.8. Минимизация прав доступа: доступ к ПД предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;

3.2.9. Гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем ПД Организации, а также объема и состава обрабатываемых ПД;

3.2.10. Специализация и профессионализм: реализация мер по обеспечению безопасности ПД осуществляется Работниками, имеющими необходимые квалификацию и опыт;

3.2.11. Эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД;

3.2.12. Наблюдаемость и прозрачность: меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

3.2.13. Непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПД, а результаты контроля постоянно анализируются.

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

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

4. Обработка персональных данных

4.1. Получение ПД

4.1.1. Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предлагаемых источниках и способах получения ПД, перечне действий с ПД, 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 ПД, создаются путем:

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

б) внесение сведений в учетные формы;

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

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

4.2. Обработка ПД

4.2.1. Обработка персональных данных осуществляется:

4.2.1.1. С согласия субъекта персональных данных на обработку его персональных данных;

4.2.1.2. В случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

4.2.1.3. 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 ПД осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Организации.

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

4.2.2. Цели обработки ПД:

4.2.2.1. Обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства Российской Федерации от 04.11. 2012 г. № 1006;

4.2.2.2. Осуществление трудовых отношений;

4.2.2.3. Осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПД следующих субъектов:

4.2.3.1. Физические лица, состоящие с учреждением в трудовых отношениях;

4.2.3.2. Физические лица, являющие близкими родственниками сотрудников учреждения;

4.2.3.3. Физические лица, уволившиеся из учреждения;

4.2.3.4. Физические лица, являющие кандидатами на работу;

4.2.3.5. Физические лица, состоящие с учреждением в гражданско-правовых отношениях;

4.2.3.6. Физические лица, обратившиеся в учреждение за медицинской помощью.

4.2.4. ПД, обрабатываемые Организацией:

4.2.4.1. Данные, полученные при осуществлении трудовых отношений;

4.2.4.2. Данные, полученные при осуществлении отборов кандидатов на работу в Организацию;

4.2.4.3. Данные, полученные при осуществлении гражданско-правовых отношений;

4.2.4.4. Данные, полученные при оказании медицинской помощи.

Полный список ПД, представлен в перечне ПД, утвержденным главным врачом Организации.

4.2.5. Обработка персональных данных ведется:

4.2.5.1. С использованием средств автоматизации;

4.2.5.2. Без использования средств автоматизации.

4.3. Хранение ПД

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

4.3.2. ПД, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа (регистрация).

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

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

4.3.5. Хранение ПД в форме, позволяющей определить субъекта ПД, 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 ПД

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

4.4.2. ПД на электронных носителях уничтожается путем стирания или форматирования носителя.

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

4.5. Передача ПД

4.5.1. Организацией передается ПД третьим лицам в следующих случаях:

4.5.1.1. Субъект выразил свое согласие на такие действия;

4.5.1.2. Передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым передаются ПД

Третьи лица, которым передаются ПД:

4.5.2.1. Пенсионный фонд РФ для учета (на законных основаниях);
4.5.2.2. Налоговые органы РФ (на законных основаниях);
4.5.2.3. Фонд социального страхования (на законных основаниях);
4.5.2.4. Территориальный фонд обязательного медицинского страхования (на законных основаниях);
4.5.2.5. Страховые медицинские организации по обязательному и медицинскому страхованию (на законных основаниях);
4.5.2.6. Банки для начисления заработанной платы (на законных основаниях);
4.5.2.7. Судебные и правоохранительные органы в случаях, установленных законодательством;
4.5.2.8. Бюро кредитных историй (с согласия субъекта);
4.5.2.9. Юридические фирмы, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта);
4.5.2.10. Иные физические и юридические лица.

5. Защита персональных данных

5.1. В соответствии в требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.
5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающие создание, функционирование и совершенствование СЗПД.
5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнёрами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.
5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.
5.5. Основными мерами защиты ПД, используемыми Организацией, являются:
5.5.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организация обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД;
5.5.2. Определение актуальных угроз безопасности ПД при их обработке ИСПД, и разработка мер и мероприятий по защите ПД;
5.5.3. Разработка политики в отношении обработки персональных данных;
5.5.4. Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечении регистрации и учета всех действий, совершаемых с ПД в ИСПД;
5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПД, обеспечение их сохранности;
5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

5.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

5.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;

5.5.10. Соблюдение условий, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПД;

5.5.11. Установление правил доступа к обрабатываемым ПД, обеспечение регистрации и учета действий, совершаемых с ПД, а также обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

5.5.12. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.5.13. Обучение работников Организации, непосредственно осуществляющих обработку персональных данных, положениями законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

5.5.14. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПД и обязанности Организации

6.1. Основные права субъекта ПД

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

6.1.1. Подтверждение факта обработки персональных данных оператором;

6.1.2. Правовые основания и цели обработки персональных данных;

6.1.3. Цели и применяемые оператором способы обработки персональных данных;

6.1.4. 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;

6.1.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6.1.6. Сроки обработки персональных данных, в том числе сроки их хранения;

6.1.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

6.1.8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;

6.1.9. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

6.1.10. Иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект ПД вправе требовать от оператора уничтожения 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:

6.2.1. При сборе ПД предоставить информацию об обработке его ПД;

6.2.2. В случаях если ПД были получены не от субъекта ПД уведомить субъекта;

6.2.3. При отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;

6.2.4. Опубликовать или иным образом обеспечить неограниченным доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;

6.2.5. Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД;

6.2.6. Давать ответы на запросы и обращения субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.

Юрисконсульт Л.А. Борисова