Государственное бюджетное учреждение
здравоохранения Архангельской области
«Архангельский психоневрологический
диспансер»

УТВЕРЖДЕНА
Приказом главного врача
ГБУЗ Архангельской области «АПНД»
Яшкович В.А. Яшкович
«19» декабря 2016
№ 76/2

Политика обработки персональных данных и реализуемых требований к защите персональных данных государственного бюджетного учреждения здравоохранения Архангельской области «Архангельский психоневрологический диспансер»

1. Общие положения

1.1. Настоящая Политика информационной безопасности обработки персональных данных (далее – Политика) разработана в соответствии с положениями Конституции РФ, Трудового кодекса РФ, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), ФЗ "Об информации, информационных технологиях и о защите информации" и иных нормативно-правовых актов, регулирующих вопросы защиты персональных данных.

1.2. Основной целью настоящей Политики является обеспечения защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную, семейную и врачебную тайну.

1.3. Настоящая Политика определяет основные вопросы, связанные с обработкой персональных данных в государственном бюджетном учреждении здравоохранения Архангельской области «Архангельский психоневрологический диспансер» (далее - Учреждение) с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

1.4. Персональные данные являются конфиденциальной, охраняемой информацией и на них распространяются все требования, установленные внутренними документами Учреждении к защите конфиденциальной информации.

1.5. В настоящей Политике используются следующие термины и определения:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъект персональных данных);
- субъект персональных данных – сотрудник Учреждения или пациент Учреждения;
- 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;
- 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;

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

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

- общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с Федеральными законами не распространяется требование соблюдения конфиденциальности.

1.3. Действие политики распространяется на все персональные данные субъектов, обрабатываемые в Учреждении с использованием средств автоматизации, а также без использования таких средств.

1.4. Настоящая Политика является общедоступной и должна иметь неограниченный доступ всех субъектов персональных данных.

2. Понятие и состав персональных данных

2.1. Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. Учреждение обрабатывает персональные данные следующих категорий субъектов персональных данных:

- персональные данные работников Учреждения - информация, необходимая Учреждению в связи с трудовыми отношениями;

- персональные данные пациентов Учреждения – информация, необходимая Учреждению для оказания квалифицированной специализированной медицинской помощи - персональные данные пациента (потенциального пациента), партнера, контрагента (потенциального контрагента), а также персональные данные руководителя, участника (акционера) или сотрудника юридического лица, являющегося пациентом или контрагентом (потенциальным пациентом, партнером, контрагентом) Учреждения - информация, необходимая Учреждению для выполнения своих обязательств в рамках уставной деятельности и договорных отношений с пациентом;

3. Цели и случаи обработки персональных данных

3.1. Целями обработки персональных данных являются:

- организация кадрового учета, ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, исполнение налогового законодательства РФ в связи с исчислением и уплатой НДФЛ, а также пенсионного законодательства РФ при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнение первичной статистической документации;

- оказание медицинских услуг пациентам в соответствии с Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее - Закон № 323-ФЗ);

- заключение, исполнение и прекращение гражданско-правовых договоров;

3.2. Обработка персональных данных в Учреждении допускается в случаях:

- если обработка персональных данных осуществляется с согласия субъекта персональных данных;

- если обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться

выгодоприобретателем или поручителем;

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

- если обработка персональных данных необходима для осуществления прав и законных интересов Учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- если обработка персональных данных необходима для осуществления научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

- если обработка персональных данных осуществляется в медицинских, исследовательских, статистических или иных целях при условии обязательного обезличивания персональных данных;

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

- если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законом;

4. Основные принципы обработки персональных данных

4.1. Обработка персональных данных возможна только в соответствии с целями, определившими их получение.

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

4.3. Право доступа для обработки персональных данных имеют сотрудники Учреждения в соответствии с возложенными на них функциональными обязанностями.

4.4. При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки.

4.5. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта 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.

4.6. Обрабатываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

4.7. Сроки хранения персональных данных определяются в соответствии со сроком действия гражданско-правовых отношений между субъектом персональных данных и Учреждением, сроком исковой давности, сроками хранения документов на бумажных носителях и документов в электронных базах данных, иными требованиями законодательства РФ, а также сроком действия согласия субъекта на обработку его персональных данных.

5. Обрабатываемые персональные данные

5.1. Учреждение осуществляет обработку персональных данных работников Учреждения с письменного согласия в случаях, установленных ст. 11 Закона № 152-ФЗ.

5.2. Обработка специальных категорий персональных данных, касающихся состояния здоровья, ведется на пациентов при оказании медицинской услуги. Обработка ведется с письменного согласия пациента в соответствии со ст. 6, 9, 10 Закона № 152-ФЗ, ч. 3 ст. 13 Закона № 323-ФЗ.

5.3. В целях информационного обеспечения в Учреждении создаются общедоступные источники персональных данных, в том числе справочники, адресные и телефонные книги. В общедоступные источники персональных данных с согласия работника могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адреса электронной почты и иные персональные данные, сообщаемые субъектом персональных

данных.

6. Права субъекта персональных данных

Субъект персональных данных имеет право:

6.1. 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 Учреждением способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением 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 Закона № 152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Законом № 152-ФЗ или другими Федеральными законами.

Получение данной информации осуществляется на основании письменного запроса субъекта персональных данных в Учреждение. Ответ, содержащий запрашиваемую информацию либо мотивированных отказ в ее предоставлении направляется субъекту по адресу, указанному в запросе, в течение 30 дней.

6.2. Требовать от Учреждения уточнения своих 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.

6.3. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством РФ.

6.4. Обжаловать в суд любые неправомерные действия или бездействие Учреждения при обработке и защите его персональных данных.

7. Обязанности организации

Учреждения обязуется:

7.1. Принимать необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.2. Осуществлять мероприятия по организационной и технической защите персональных данных в соответствии с требованиями законодательства РФ по вопросам обработки персональных данных.

7.3. В целях обеспечения защиты персональных данных проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения безопасности их персональных данных, а также определять актуальные угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

7.4. При выявлении актуальных угроз применять необходимые и достаточные правовые, организационные и технические меры по обеспечению безопасности персональных данных, включающие в себя:

- определение угроз безопасности информации, содержащей персональные данные, при ее обработке;
- применение организационных и технических мер по обеспечению безопасности информации, содержащей персональные данные, при ее обработке;
- оценку эффективности принимаемых мер до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей информации, содержащей персональные данные;
- обнаружение фактов несанкционированного доступа к информации, содержащей персональные данные, и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к информации, содержащей персональные данные, обеспечение регистрации и учета всех действий, совершаемых с информацией, содержащей персональные данные, в информационной системе персональных данных;
- контроль за принимаемыми мерами.

7.5. Учреждение обязуется отвечать на запросы субъектов персональных данных, их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в части обрабатываемых персональных данных в соответствии с требованиями законодательства.

7.6. В случае предоставления субъектом персональных данных либо его представителем сведений, подтверждающих факты каких-либо нарушений в процессе обработки персональных данных, Учреждение обязуется устранить данные нарушения в течение семи рабочих дней и уведомить субъекта персональных данных о внесенных изменениях и принятых мерах.

8. Обязанности и ответственность сотрудников организации

8.1. Сотрудники Учреждения, допущенные к обработке персональных данных, обязаны:

- знать и неукоснительно выполнять требования настоящей Политики;
- обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;
- не разглашать персональные данные, полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;
- пресекать действия третьих лиц, которые могут привести к разглашению (уничтожению, искажению) персональных данных;
- выявлять факты разглашения (уничтожения, искажения) персональных данных и информировать об этом непосредственного руководителя;
- хранить тайну о сведениях, содержащих персональные данные в соответствии с локальными актами Учреждения.

8.2. Сотрудникам Учреждения, допущенным к обработке персональных данных, запрещается несанкционированное и нерегламентированное копирование персональных данных на бумажные носители информации и на любые электронные носители информации, не предназначенные для хранения персональных данных.

8.3. Каждый новый работник Учреждения, непосредственно осуществляющий обработку персональных данных, подлежит ознакомлению с требованиями законодательства РФ по обработке и обеспечению безопасности персональных данных, с настоящей Политикой и другими локальными актами по вопросам обработки и обеспечения безопасности персональных данных и обязуется их соблюдать.

8.4. Лица, виновные в нарушении требований законодательства РФ в области персональных данных, несут дисциплинарную, материальную, гражданско-правовую, административную или уголовную ответственность.

9. Условия обработки персональных данных, их хранения и передачи третьим лицам

9.1. Обработка персональных данных:

9.1.1. Работники Учреждения, допущенные к обработке персональных данных на основании правовых актов Учреждения и должностных регламентов, осуществляют обработку персональных данных после ознакомления с нормативными актами Учреждения, регламентирующими порядок и процедуры работы с персональными данными.

9.1.2. Доступ к персональным данным работников имеют:

- руководители структурных подразделений (к данным работников своего подразделения)
- специалисты отдела кадров и бухгалтерии – к тем данным, которые необходимы им для выполнения конкретных функций.

9.2. Хранение персональных данных:

9.2.1. Персональные данные хранятся в электронном виде в составе информационных систем персональных данных (далее – ИСПДн), в составе архивных копий баз данных ИСПДн и на бумажных носителях.

9.2.2. При обработке и хранении персональных данных соблюдаются организационные меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним, к которым относятся:

- назначение работника Учреждения, ответственного за организацию обработки персональных данных, и за обеспечение безопасности персональных данных при их обработке в ИСПДн;
- ограничение физического доступа к местам хранения персональных данных в бумажном виде и носителях информации в электронном виде;
- соблюдение правил обработки персональных данных в ИСПДн;
- применение сертифицированных средств защиты информации.

9.3. Передача персональных данных:

9.3.1. Для достижения целей обработки персональных данных субъектов, Учреждение может передавать персональные данные третьим лицам:

1) Персональные данные работников Учреждения:

В соответствии с требованиями Трудового Кодекса РФ (Закон № 197-ФЗ) только с от 30.12.2001 письменного согласия работника (ст. 88);

- в Федеральную инспекцию по труду (ст. 357 Трудового Кодекса РФ);
- в органы государственного контроля и надзора за соблюдением законов о труде (ст. 357, 366-369 Трудового Кодекса РФ);
- в Пенсионный фонд (Закон № 27-ФЗ от 01.04.1996 г.);
- в Фонд социального страхования (Закон № 125-ФЗ от 24.07.1998 г.);
- в налоговые органы (ст. 24 Налогового кодекса РФ);
- в рамках договора (контракта), предусматривающего обеспечение конфиденциальности и безопасности полученных сведений (банки (ст. 136 Трудового Кодекса РФ), страховые компании, организации, осуществляющие сопровождение ИСПДн).

2) Персональные данные пациентов:

- при поступлении запросов от уполномоченных государственных органов, в рамках действующего законодательства (пункт 3, части 4, ст. 13 Закона № 323-ФЗ»).

10. Меры по обеспечению безопасности персональных данных

10.1. При обработке персональных данных Учреждения принимает необходимые правовые, организационные и технические меры защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

10.2. Обеспечение безопасности персональных данных достигается, в частности:

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых

обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием необходимых мер;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационной системы персональных данных.

10.3 Определение угроз безопасности персональных данных, разработка на их основе частной модели угроз безопасности персональных данных и разработка системы защиты персональных данных для соответствующего класса ИСПДн;

10.4. Реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;

10.5. Применение сертифицированных средств защиты информации;

10.8. Осуществление антивирусного контроля;

10.9. Парольная защита доступа к ИСПДн;

10.10. Разработка и утверждение локальных актов Учреждения, регламентирующих порядок обработки персональных данных, разработка инструкций;

10.11. Обучение работников Учреждения, допущенных к обработке персональных данных, и использующих средства защиты информации, правилам работы с ними;

10.12. Проведение периодических проверок состояния защищенности ИСПДн.

11. Заключительные положения

11.1. Действующая редакция Политики на бумажном носителе хранится в общем отделе, отделе кадров Учреждения.

11.2. Электронная версия действующей редакции Политики общедоступна на сайте Учреждения в сети Интернет http: //29apnd.ru.

11.3. При внесении изменений в заголовке Политики указывается дата утверждения действующей редакции Политики.

11.4. Политика актуализируется и заново утверждается на регулярной основе – не реже одного раза в три года с момента ее опубликования.

11.5. Политика может актуализироваться и заново утверждаться ранее срока, указанного в п. 9.4 настоящей Политики, по мере внесения изменений в нормативные правовые акты в сфере персональных данных или в локальные акты, регламентирующие организацию обработки и обеспечение безопасности персональных данных.