

РЕСПУБЛИКА КАРЕЛИЯ
МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КАРЕЛИЯ
РЕСПУБЛИКАНСКИЙ НАРКОЛОГИЧЕСКИЙ ДИСПАНСЕР

П Р И К А З

«07» октября 2022 года

№ 158

г. Петрозаводск

«Об утверждении Политики в отношении персональных данных»

В соответствии с п. 2 статьи 18.1 Федерального закона от 27 июля 2006 года № 152 «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить «Политику в отношении персональных данных Государственного бюджетного учреждения здравоохранения Республики Карелия «Республиканский наркологический диспансер» (далее – Политика).
2. Считать утратившей силу Политику, утвержденную главным врачом ГБУЗ «РНД» О.С. Ларионовой 20.12.2018 г.
3. Назначить ответственным за исполнение Политики инженера по защите информации Листопадова А.М.
4. Контроль над исполнением приказа оставляю за собой.

Главный врач



О.С. Ларионова

Приложение 1
к приказу ГБУЗ «РНД»
от «07» октября 2022 г. № 158

ПОЛИТИКА

**в отношении обработки персональных данных
Государственного бюджетного учреждения здравоохранения Республики Карелия
«Республиканский наркологический диспансер»**

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	3
2. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ	4
3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	5
4. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ:	5
5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	6
6. ПРАВА СУБЪЕКТА НА ДОСТУП И ИЗМЕНЕНИЕ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ	7
7. ОБЯЗАННОСТИ ГБУЗ «РНД»	7
7. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБУЗ «РНД»	9
8. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРИНИМАЕМЫЕ В ГБУЗ «РНД»	10
9. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГБУЗ «РНД».....	10
10. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПДН ГБУЗ «РНД»	10

1. Общие положения

Политика в отношении обработки персональных данных (далее - Политика) государственного бюджетного учреждения здравоохранения Республики Карелия «Республиканский наркологический диспансер» (далее - ГБУЗ «РНД») разработана в соответствии с п. 2 статьи 18.1 Федерального закона от 27 июля 2006 года № 152 «О персональных данных» и определяет деятельность ГБУЗ «РНД» в отношении обработки информации о субъектах персональных данных.

Политика определяет основные цели и задачи, основные требования к уровням безопасности информации, а также требования к сотрудникам, являющимся пользователями информационных систем персональных данных (далее - ИСПДн) в ГБУЗ «РНД».

Политика разработана и определяет проведение комплекса системных мероприятий по обеспечению информационной безопасности, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных (далее – ПДн) с применением технических и организационных мер средств защиты.

Под информационной безопасностью ПДн понимается защищенность ПДн в обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ГБУЗ «РНД», мер по выявлению, отражению и ликвидации последствий реализации различных видов угроз ПДн в ГБУЗ «РНД».

Настоящая Политика разработана в соответствии с положениями следующих нормативных правовых актов:

Конституция Российской Федерации (принята всенародным голосованием 12.12.1993); Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;

Федеральный закон от 21.11.2011 № 323-ФЗ «Об охране здоровья граждан в Российской Федерации»;

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утв. Постановлением Правительства Российской Федерации от 01.11.2012 № 1119);

«Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (утв. Постановлением Правительства Российской Федерации от 15.09.2008 № 687);

«Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в

области персональных данных» (утв. Приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312);

«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. Приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21); «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (утв. Приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378).

В целях реализации настоящей Политики в ГБУЗ «РНД» утверждены:

- положение по защите персональных данных;
- перечень персональных данных, обрабатываемых в ГБУЗ «РНД» в связи с реализацией трудовых отношений, а также в связи с оказанием медицинской помощи;
- перечень информационных систем персональных данных используемых в ГБУЗ «РНД»; модели угроз и модель нарушителя безопасности персональных данных при их обработке в информационных системах персональных данных ГБУЗ «РНД»;
- должностная инструкция ответственного за организацию обработки персональных данных;
- инструкция пользователя информационных систем персональных данных;
- инструкция администратора безопасности информационных систем персональных данных;
- иные локальные документы ГБУЗ «РНД», принимаемые во исполнение требований действующих нормативных правовых актов Российской Федерации и Республики Карелия в области обработки персональных данных.

Действие настоящей Политики распространяется на все процессы в ГБУЗ «РНД» в рамках которых осуществляется обработка персональных данных, как с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, так и без использования таких средств.

Использование услуг ГБУЗ «РНД» означает согласие субъекта ПДн с настоящей Политикой и указанными в ней условиями обработки его ПДн.

Настоящая Политика вступает в силу с момента ее утверждения главным врачом ГБУЗ «РНД» и действует бессрочно до замены ее новой Политикой. Обеспечение неограниченного доступа к Политике реализуется путем ее публикации на сайте Оператора в сети Интернет, либо иным способом.

2. Основные понятия и определения

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

Субъект персональных данных – физическое лицо, индивидуальный предприниматель или представитель юридического лица, заключившее с Оператором гражданский договор на выполнение работ, оказание услуг в соответствии с осуществляемыми Оператором видами деятельности, а также работники Оператора и работники контрагентов Оператора.

Оператор персональных данных - государственное бюджетное учреждение здравоохранения «Республиканский наркологический диспансер» (далее - ГБУЗ «РНД») организующее и осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе: сбор; запись; систематизацию; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передачу (распространение, предоставление, доступ); обезличивание; блокирование; удаление; уничтожение.

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;

3. Цели обработки персональных данных

ГБУЗ «РНД» производит обработку только тех ПДн, которые необходимы для:

- осуществления, в рамках законодательства Российской Федерации, возложенных Министерством здравоохранения Республики Карелия на ГБУЗ «РНД» функций, полномочий и обязанностей;
- выполнения требований законодательства в сфере труда и налогообложения;
- ведения текущего бухгалтерского и налогового учёта, формирование, изготовления и своевременной подаче бухгалтерской, налоговой и статистической отчётности;
- выполнения требований законодательства по определению порядка обработки и защиты ПДн граждан, являющихся пациентами ГБУЗ «РНД»;
- иных законных целей.

4. Категории субъектов персональных данных:

В ГБУЗ «РНД» обработке подлежат ПДн следующих категорий субъектов ПДн:

- сотрудники и бывшие сотрудники, кандидаты на вакантные должности;

- контрагенты ГБУЗ «РНД»;
- физические лица, обратившиеся в ГБУЗ «РНД» в порядке, установленном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»;
- физические лица, обратившиеся за медицинской помощью или направленные на лечение по решению суда.

Категории субъектов персональных данных ГБУЗ «РНД»	Перечень персональных данных, обрабатываемых ГБУЗ «РНД»
сотрудники и бывшие сотрудники, кандидаты на вакантные должности	Фамилия, имя, отчество, пол, возраст, дата и место рождения, адрес места жительства, состояние здоровья (сведения прохождения медицинских осмотров), семейное положение, ФИО детей и дата их рождения, образование, паспортные данные, выполняемая работа с начала трудовой деятельности, номер телефона и адрес электронной почты, отношение к воинской службе, ИНН, СНИЛС, сведения о доходах и задолженностях
Контрагенты в ГБУЗ «РНД»	паспортные данные, юридические документы
Физические лица, обратившиеся в ГБУЗ «РНД» в порядке, установленном Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации»	Фамилия, имя, отчество, адрес места жительства номер телефона и адрес электронной почты, иные данные, указанные в обращении
Физические лица, обратившиеся для оказания медицинской помощи или направленные на лечение по решению суда	Фамилия, имя, отчество, пол, возраст, дата и место рождения, адрес места жительства, состояние здоровья, семейное положение, образование, паспортные данные, ИНН, СНИЛС, специальные данные (результаты анализов и исследований)

5. Порядок и условия обработки персональных данных

ГБУЗ «РНД» обрабатывает и хранит ПДн субъектов в соответствии с внутренними нормативными документами, разработанными согласно законодательству РФ. В отношении ПДн субъекта обеспечивается их конфиденциальность, целостность и доступность.

В ГБУЗ «РНД» обработка ПДн осуществляется на бумажных носителях и в автоматизированном виде.

Перечень действий, совершаемых ГБУЗ «РНД» с персональными данными субъектов: сбор данных, накопление, хранение, передача, актуализация, систематизация, уничтожение.

При достижении целей обработки ПДн, а также в случае отзыва субъектом ПДн согласия на их обработку, ПДн подлежат уничтожению, если:

иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн;

иное не предусмотрено иным соглашением между ГБУЗ «РНД» и субъектом ПДн.

ГБУЗ «РНД» не вправе осуществлять обработку без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или иными федеральными законами.

6. Права субъекта на доступ и изменение его персональных данных

Для обеспечения соблюдения установленных законодательством прав субъектов ПДн в ГБУЗ «РНД» введен порядок работы с обращениями и запросами субъектов ПДн, предоставления субъектам ПДн установленной законом информации.

Данный порядок обеспечивает соблюдение следующих прав субъектов ГБУЗ «РНД»:

1) право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн;
- правовые основания и цели обработки ПДн;
- цели и применяемые способы обработки ПДн;
- наименование и место нахождения ГБУЗ «РНД», сведения о лицах (за исключением работников ГБУЗ «РНД»), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с ГБУЗ «РНД» или на основании Федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению ГБУЗ «РНД», если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

2) право на уточнение, блокирование или уничтожение своих ПДн, которые являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных целей обработки.

7. Обязанности ГБУЗ «РНД»

В соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных» ГБУЗ «РНД» обязан:

- 1) осуществлять обработку ПДн с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных»;
- 2) не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ «О персональных данных»;
- 3) предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, в соответствии с которыми такое согласие не требуется;
- 4) в случаях, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных» осуществлять обработку персональных данных только с согласия в письменной форме субъекта ПДн;
- 5) предоставлять субъекту ПДн по его запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ в предоставлении указанной информации и дать в письменной форме мотивированный ответ, содержащий ссылку на положения Федерального закона № 152-ФЗ «О персональных данных», являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. При обращении либо при получении запроса субъекта ПДн или его представителя предоставить субъекту ПДн или его представителю информацию, касающуюся обработки его ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.
- 6) если предоставление ПДн является обязательным в соответствии с Федеральным законом, разъяснить субъекту ПДн юридические последствия отказа предоставить его персональные данные;
- 7) принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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 ПДн. Описание принимаемых мер приведено в п. 9 настоящей Политики;
- 8) по требованию субъекта ПДн внести изменения в обрабатываемые ПДн, или уничтожить их, если ПДн являются неполными, неточными, неактуальными, незаконно полученными или не являются необходимыми для заявленной цели обработки в срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих указанные факты, а также уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы. Вести Журнал учета обращений субъектов ПДн, в котором должны фиксироваться запросы субъектов ПДн на получение ПДн, а также факты предоставления ПДн по этим запросам.
- 9) уведомлять субъекта ПДн об обработке ПДн в том случае, если ПДн были получены не от субъекта ПДн. Исключение составляют следующие случаи:
 - субъект ПДн уведомлен об осуществлении обработки его ПДн ГБУЗ «РНД»;
 - персональные данные получены ГБУЗ «РНД» на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- предоставление субъекту ПДн сведений, содержащихся в Уведомлении об обработке персональных данных, нарушает права и законные интересы третьих лиц.

10) в случае выявления неправомерной обработки ПДн или неточных персональных данных, устранить выявленные нарушения в соответствии с порядком и сроками, установленными Федеральным законом № 152-ФЗ «О персональных данных»;

11) в случае достижения целей обработки ПДн незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между ГБУЗ «РНД» и субъектом ПДн либо, если ГБУЗ «РНД» не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных №152-ФЗ «О персональных данных» или другими Федеральными законами.

12) в случае отзыва субъектом ПДн согласия на обработку своих ПДн прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между ГБУЗ «РНД» и субъектом персональных данных. Об уничтожении персональных данных ГБУЗ «РНД» обязан уведомить субъекта ПДн.

8. Обеспечение безопасности персональных данных в ГБУЗ «РНД»

Безопасность ПДн достигается путем:

- определение угроз безопасности персональных данных при их обработке в ИСПДн;
- выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- применения организационных и технических мер для исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий;
- своевременного обнаружения, реагирования на угрозы безопасности ПДн;
- применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- учета машинных носителей ПДн;
- оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- установления доступа к ИСПДН только для авторизованных пользователей;
- предотвращения преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных;
- обязательным выполнением положений настоящей Политики всеми сотрудниками ГБУЗ «РНД»;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

9. Организационные и технические меры по защите персональных данных, принимаемые в ГБУЗ «РНД»

В ГБУЗ «РНД» принимаются следующие меры:

издание локальных нормативных актов и утверждение документов по организации обработки ПДн;

- назначение администратора безопасности ПДн;
- определение должностных обязанностей сотрудников, осуществляющих обработку ПДн;
- оборудование охранной, пожарной сигнализации, системы видеонаблюдения;
- хранение документов с ПДн на бумажных носителях в защищенных помещениях с ограниченным доступом и кругом лиц;
- использование антивирусных средств защиты информации, сертифицированных ФЭСТЭК России и ФСБ России;
- идентификация и проверка подлинности пользователей при входе в операционную систему и в информационные системы;
- использование сертифицированных ФСБ России средств криптографической защиты информации при взаимодействии и передаче данных между оператором и информационной системой по сети Интернет.

10. Контроль эффективности системы защиты персональных данных в ГБУЗ «РНД»

Контроль эффективности системы защиты ИСПДн осуществляется ГБУЗ «РНД» с периодичностью раз в полугодие. Целью контроля является своевременное выявление ненадлежащих режимов работы ИСПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администратором безопасности с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным действующим законодательством Российской Федерации требованиям.

11. Ответственность пользователей информационных систем ПДн ГБУЗ «РНД»

В соответствии со ст.24 Законом №152-ФЗ лица, виновные в нарушении требований Закона №152-ФЗ, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного кодекса Российской Федерации).

Администратор безопасности несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками ГБУЗ «РНД» - пользователями ИСПДн правил, связанных с безопасностью ПД, они несут ответственность, установленную действующим законодательством Российской Федерации