

Приложение № 1
к приказу № 526 от 27.09.2023 г.

УТВЕРЖДАЮ
Главный врач
ГБУЗ ВО «ГБ № 4 г. Владимира»



В.Е. Савинов

«27» сентября 2023 г.

ПОЛИТИКА ГБУЗ ВО «ГБ № 4 г. ВЛАДИМИРА» В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая Политика государственного бюджетного учреждения здравоохранения Владимирской области «Городская больница №4 г.Владимира» (далее – Учреждение, Оператор) в отношении обработки персональных данных (далее – Политика) разработана:

- во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных, Закон о ПД),
- в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установления ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Настоящая Политика:

- действует в отношении всех персональных данных, которые обрабатывает Учреждение,
- определяет общий порядок, принципы и условия обработки Оператором персональных данных физических лиц: 1) в связи с реализацией трудовых отношений (кадрового состава), 2) осуществлением уставной деятельности, 3) при обращении за медицинской помощью в Учреждение, 4) а также персональных данных, обрабатываемых в процессе исполнения договорных обязательств или в повседневной деятельности, и обеспечивает защиту прав субъектов персональных данных при обработке их персональных данных.

1.3. Настоящая Политика распространяется на:

- отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики,
- все структурные подразделения Учреждения, участвующие в обработке персональных данных.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных с целью обеспечения неограниченного доступа к документу настоящая Политика размещается в свободном доступе, в том числе:

- на локальных дисках – для возможности ознакомления работников учреждения,
- на информационных стендах – для ознакомления пациентов Учреждения,
- на официальном сайте учреждения (в случае необходимости и при условии получения/обработки персональных данных через сайт).

1.5. Основные понятия, используемые в Политике:

персональные данные (ПД) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Персональные данные относятся к категории конфиденциальной информации и защищены от несанкционированного, в том числе случайного, доступа к ним.

персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения установленном порядке;

общедоступные персональные данные - персональные данные, доступ неограниченного

круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

субъект персональных данных (субъект ПД) - физическое лицо, которое прямо или косвенно определено или определяется с помощью персональных данных;

оператор персональных данных (Оператор) - государственное бюджетное учреждение здравоохранения Владимирской области «Городская больница №4 г.Владимира» (Учреждение), самостоятельно или совместно с другими лицами организующее и/или 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;

использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных, либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях, на сайте Учреждения и соцсетях или предоставление доступа к персональным данным каким-либо иным способом;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки (сбора, систематизации, накопления, использования, распространения, передачи) 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;

конфиденциальность персональных данных - обязательное для оператора и иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных или иного законного основания;

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, и являющееся субъектом персональных данных;

медицинская деятельность – уставная деятельность Учреждения по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с обращением донорской крови и/или ее компонентов в медицинских целях;

лечащий врач – работник Учреждения, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения, непосредственно участвует в сборе персональных данных.

2. Правовые основания обработки персональных данных

2.1. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе:

- Конституция Российской Федерации,
- Трудовой кодекс Российской Федерации,
- Гражданский кодекс Российской Федерации,
- Налоговый кодекс Российской Федерации,
- Кодекс Российской Федерации об административных правонарушениях,
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»,
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»,
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»,
- постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- постановление Правительства РФ от 16.01.2023 № 24 «Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрете или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан»,
- постановление Правительства РФ от 11.05.2023 № 736 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг, внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившим силу постановления Правительства Российской Федерации от 4 октября 2012 г. № 1006»,
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»,
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»,
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и

массовых коммуникаций от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»,

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

- приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Составы и содержания 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»,

- приказ ФСБ России от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»,

- иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Учреждения.

2.2. Правовым основанием обработки персональных данных также являются:

- устав Учреждения.
- договоры, заключаемые между Учреждением и субъектами персональных данных;
- согласие субъектов персональных данных на обработку их персональных данных (работников и пациентов Учреждения),
- согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

3. Основные права и обязанности Учреждения и субъекта персональных данных

3.1. Учреждение обязано:

3.1.1. организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;

3.1.2. отвечать на обращения и запросы субъектов ПД и их законных представителей в соответствии с требованиями Закона о персональных данных;

3.1.3. сообщать в уполномоченный орган по защите прав субъектов ПД (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию в течение 10 (десять) рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на 5 (пять) рабочих дней. Для этого Учреждение направляет в Роскомнадзор мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации;

3.1.4. в порядке, определенном Роскомнадзором, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование его о компьютерных инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных.

3.2. Учреждение имеет право:

3.2.1. самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

3.2.2. поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании

заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных, и не обязано получать согласие субъекта на обработку его персональных данных;

3.2.3. в случае отзыва субъектом ПД согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта ПД при наличии оснований, указанных в Законе о персональных данных.

3.3. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе без принуждения или введения в заблуждение с чьей-либо стороны.

3.4. Субъект персональных данных имеет право:

3.4.1. получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами.

Сведения предоставляются субъекту ПД Учреждением в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПД, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных.

3.4.2. требовать от Учреждения 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.

3.4.3. обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

3.5. Запрещается принимать на основании исключительно автоматизированной обработки персональных данных решения, порождающие юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

4. Принципы и условия обработки персональных данных

4.1. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

- наличие законных оснований для обработки персональных данных;
- законность и справедливость целей и способов обработки;
- ограниченность обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопущение обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущение обработки избыточных персональных данных по отношению к заявленным целям их обработки;
- недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых между собой целях;
- обработка только тех персональных данных, которые отвечают целям их обработки;
- соответствие содержания и объема (недопущение избыточности) обрабатываемых персональных данных заявленным целям обработки;
- обеспечение точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;
- 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 законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- уничтожение либо обезличивание персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей.

4.2. Обработка персональных данных в Учреждение может осуществляться в следующих случаях:

- получено согласие субъекта на обработку его персональных данных;
- обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных осуществляется в связи с участием субъекта ПД в гражданском и арбитражном судопроизводстве;
- обработка персональных данных необходима для исполнения судебного акта в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПД, а также для заключения договора по инициативе субъекта ПД;
- 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 прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;
- обработка персональных данных производится в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации,
- производится обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (общедоступные данные).

4.3. Учреждение и работники, получившие доступ к персональным данным в силу трудовых обязанностей, обязаны соблюдать конфиденциальность (не раскрывать третьим лицам и не распространять) персональных данных без согласия субъекта ПД, если иное не предусмотрено федеральным законом.

5. Цели сбора и обработки персональных данных

5.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

5.3. Обработка Оператором персональных данных осуществляется в следующих целях:

5.3.1. осуществление Учреждением своей деятельности в соответствии с уставом:

✓ оказание медицинской помощи/медицинских услуг пациентам, в том числе идентификация пациентов (их законных представителей, заказчиков), медико-профилактические цели (установление медицинского диагноза, оказание медицинских услуг, контроль качества оказания медицинской помощи и др.), отражение информации в медицинской документации (обработка сведений, составляющих врачебную тайну), исполнение договора на оказание медицинских услуг, предоставление сведений страховым компаниям и установленной законодательством отчетности в отношении оказанных медицинских услуг (сбор и передача статистических данных в сфере здравоохранения),

✓ заключение, исполнение и прекращение договоров с контрагентами.

5.3.2. исполнение трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе: содействие работникам в трудоустройстве, получении образования и продвижении по службе, привлечение и отбор кандидатов на работу в Учреждении, обеспечение личной безопасности работников, контроль количества и качества

выполняемой работы, обеспечение сохранности имущества, ведение кадрового и бухгалтерского учета, выплата заработной платы и иных, причитающихся работнику в соответствии с законодательством РФ или договором выплат, налоговые и социальные отчисления, заполнение и передача в уполномоченные органы требуемых форм отчетности, организация постановки на индивидуальный (персонифицированный) учет работников в системах обязательного пенсионного страхования и обязательного социального страхования.

5.3.3. осуществление пропускного режима.

5.3.4. выполнение требований действующего законодательства.

5.3.5. в иных случаях, установленных в законе, уставе Учреждения.

5.4. Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

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

5.6. 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. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

6.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разд. 5 настоящей Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6.2. Учреждение может обрабатывать персональные данные следующих категорий субъектов персональных данных:

✓ Работники Учреждения, бывшие работники, кандидаты на трудоустройство, а также члены семьи работников,

✓ Пациенты, законные представители пациентов.

✓ Прочие клиенты и контрагенты Учреждения (физические лица).

✓ Представители/работники клиентов и контрагентов Учреждения (юридических лиц).

6.3. Учреждение обрабатывает следующие категории персональных данных субъектов ПД, указанных в пункте 6.2 настоящей Политики, в зависимости от категории субъекта ПД:

6.3.1. Кандидаты для приема на работу в Учреждение - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, осуществления пропускного режима:

✓ фамилия, имя, отчество (при наличии);

✓ пол;

✓ гражданство;

✓ дата и место рождения;

✓ контактные данные (телефон, адрес электронной почты);

✓ сведения об образовании, опыте работы, квалификации;

✓ иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

6.3.2. Работники и бывшие работники Учреждения - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе для предоставления гарантий, компенсаций и мер социальной поддержки, исполнения требований законодательства РФ в области налогового и бухгалтерского учета, в том числе осуществления расчетов с работниками, оформления первичных учетных документов, осуществления пропускного режима:

✓ фамилия, имя, отчество (при наличии);

✓ пол;

✓ гражданство;

✓ дата и место рождения;

✓ изображение (фотография);

✓ паспортные данные или данные документа, удостоверяющего личность;

✓ адрес регистрации по месту жительства;

- ✓ адрес фактического проживания;
- ✓ контактные данные (телефон, адрес электронной почты);
- ✓ индивидуальный номер налогоплательщика;
- ✓ страховой номер индивидуального лицевого счета (СНИЛС);
- ✓ сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
- ✓ сведения о профессии и должности, занимаемой/ ранее занимаемых работником;
- ✓ семейное положение, наличие детей, родственные связи;
- ✓ сведения о трудовой деятельности, в том числе наличие наград, почетных званий, поощрений, награждений и (или) дисциплинарных взысканий;
- ✓ сведения о стаже работы, в том числе в медицинских учреждениях и по занимаемой должности;
- ✓ данные о регистрации брака;
- ✓ сведения о воинском учете;
- ✓ сведения о судимостях;
- ✓ сведения об инвалидности либо состоянии здоровья, влияющие на выполнение трудовой функции (осуществляется в отдельных случаях в соответствии с законодательством Российской Федерации о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации);
- ✓ сведения об удержании алиментов;
- ✓ сведения о доходе, в том числе с предыдущего места работы;
- ✓ табельный номер;
- ✓ сведения о социальных гарантиях;
- ✓ иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

6.3.3. Члены семьи работников Учреждения - для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе для предоставления гарантий, компенсаций и мер социальной поддержки работнику либо члену семьи работника (в том числе в случае смерти работника):

- ✓ фамилия, имя, отчество (при наличии);
- ✓ степень родства;
- ✓ дата и место рождения;
- ✓ серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе;
- ✓ серия и номер свидетельства о заключении брака, сведения о выдаче указанного документа и выдавшем его органе;
- ✓ иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства либо с целью получения мер социальной поддержки, в том числе в целях получения компенсации найма жилого помещения.

6.3.4. Пациенты Учреждения, в том числе потребители медицинских услуг, законные представители пациентов/ потребителей медицинских услуг – для целей оказания медицинских и медико-социальных услуг, в том числе идентификации пациента; заключения, исполнения и прекращения договоров на оказание услуг; оказания платных и бесплатных услуг субъектам персональных данных; постановки диагноза; лекарственного обеспечения; экспертизы временной нетрудоспособности; улучшения качества оказываемых услуг; осуществления связи с субъектами ПД для направления уведомлений, информации, запросов, связанных с деятельностью Учреждения; обработки обращений, заявлений, жалоб и иных сообщений субъекта ПД; проведение статистических и иных исследований на основе обезличенных персональных данных; и др., осуществления пропускного режима:

- ✓ фамилия, имя, отчество (при наличии);
- ✓ пол;
- ✓ возраст;
- ✓ дата и место рождения;
- ✓ гражданство;
- ✓ паспортные данные или данные документа, удостоверяющего личность;
- ✓ адрес регистрации по месту жительства;

- ✓ адрес фактического проживания;
- ✓ контактные данные (телефон, адрес электронной почты);
- ✓ страховой номер индивидуального лицевого счета (СНИЛС);
- ✓ номер полиса обязательного (добровольного) медицинского страхования;
- ✓ индивидуальный номер налогоплательщика (при оформлении справок для оформления налогового вычета);
- ✓ данные о состоянии здоровья, в том числе биометрические персональные данные, наличии или отсутствии заболеваний, случаях обращения за медицинской помощью;
- ✓ факт обращения в Учреждение за медицинской помощью;
- ✓ семейное и социальное положение;
- ✓ тип занятости;
- ✓ место работы;
- ✓ должность
- ✓ иные персональные данные, предоставляемые пациентом в соответствии с законодательством в сфере охраны здоровья и постановлением Правительства РФ от 11.05.2023 № 736 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг, внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившим силу постановления Правительства Российской Федерации от 4 октября 2012 г. № 1006»;
- ✓ сведения о документе, который подтверждает полномочия представителя.

6.3.5. Контрагенты и прочие клиенты Учреждения (физические лица) - для целей осуществления своей деятельности в соответствии с уставом; исполнения требований законодательства РФ в области бухгалтерского и налогового учета, в том числе осуществления расчетов с субъектами ПД, оформления первичных учетных документов, проявления должной осмотрительности, осуществления пропускного режима:

- ✓ фамилия, имя, отчество;
- ✓ пол;
- ✓ дата и место рождения;
- ✓ возраст;
- ✓ паспортные данные или данные документа, удостоверяющего личность;
- ✓ адрес регистрации по месту жительства;
- ✓ контактные данные (телефон, адрес электронной почты);
- ✓ замещаемая должность;
- ✓ индивидуальный номер налогоплательщика;
- ✓ номер расчетного счета;
- ✓ иные персональные данные, предоставляемые клиентами и контрагентами (физическими лицами), необходимые для заключения и исполнения договоров.

6.3.6. Представители (работники) клиентов и контрагентов Учреждения (юридических лиц) - для целей осуществления своей деятельности в соответствии с уставом Учреждения, осуществления пропускного режима:

- ✓ фамилия, имя, отчество;
- ✓ паспортные данные;
- ✓ контактные данные;
- ✓ замещаемая должность;
- ✓ сведения о документе, который подтверждает полномочия представителя;
- ✓ иные персональные данные, предоставляемые представителями (работниками) клиентов и контрагентов, необходимые для заключения и исполнения договоров.

6.4. Обработка Учреждением биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) осуществляется в соответствии с законодательством Российской Федерации.

6.5. Учреждением не осуществляется обработка специальных категорий персональных данных, касающихся политических взглядов, религиозных или философских убеждений и др., за исключением случаев, предусмотренных законодательством РФ.

7. Согласие на обработку персональных данных

7.1. Обработка персональных данных осуществляется:

- Учреждением в соответствии с требованиями законодательства Российской Федерации,
- с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации,
- после принятия необходимых мер по защите персональных данных.

7.2. Оператор не вправе обрабатывать персональные данные субъекта ПД без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О персональных данных».

7.3. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

7.4. Письменное согласие субъекта персональных данных должно включать:

- фамилию, имя, отчество;
- наименование и адрес Учреждения/Оператора;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;
- срок, в течение которого действует согласие;
- способ его отзыва;
- подпись субъекта персональных данных.

7.5. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его ПД третьим лицам получено от него в письменном виде при заключении договора с Учреждением, а также в случаях, установленных федеральным законом.

7.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Такое согласие предоставляется только работниками Учреждения, в том числе с целью размещения информации о них на официальном сайте и информационных стендах Учреждения.

8. Порядок, условия и способы обработки персональных данных

8.1. При обработке персональных данных в Учреждении осуществляются следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

8.2. Учреждение осуществляет обработку персональных данных для каждой цели их обработки следующими способами:

- ✓ неавтоматизированная обработка персональных данных;
- ✓ автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- ✓ смешанная обработка персональных данных.

8.3. В целях обеспечения сохранности и конфиденциальности персональных данных к обработке персональных данных допускаются работники Учреждения, в должностные обязанности которых входит обработка персональных данных. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

8.4. Обработка персональных данных для каждой цели обработки, указанной в п. 5.3 Политики, осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно от субъектов ПД или его представителя, наделенного соответствующими полномочиями;
- внесения персональных данных в журналы, реестры и информационные системы

Учреждения;

- использования иных способов обработки персональных данных.

8.5. Сбор персональных данных:

8.5.1. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Учреждение обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

8.5.2. Сбор персональных данных осуществляется непосредственно у самого субъекта ПД. Если предоставление персональных данных и/или получение Учреждением согласия на обработку персональных данных являются обязательными в соответствии с законодательством Российской Федерации, субъекту ПД разъясняются юридические последствия отказа в предоставлении таких данных и/или согласия на их обработку.

8.5.3. Получение персональных данных у иных лиц возможно только при наличии законных оснований. При получении персональных данных у иных лиц, за исключением случаев, когда персональные данные получены в рамках поручения на обработку персональных данных или когда согласие получено передающей стороной, необходимо уведомить об этом субъекта.

8.5.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечивается запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

8.5.5. В случае подтверждения факта неточности персональных данных, такие персональные данные подлежат актуализации в течение 7 (семи) рабочих дней.

8.5.6. В случае выявления факта неправомерности обработки персональных данных, такие персональные данные подлежат уничтожению в 3-дневный срок.

8.6. Передача персональных данных:

8.6.1. Передача персональных данных третьему лицу осуществляется только с согласия субъекта персональных данных или в случаях, прямо предусмотренных законодательством Российской Федерации.

8.6.2. Передача персональных данных органу государственной власти, органу местного самоуправления, органу безопасности и правопорядка, органам дознания и следствия, в Федеральную налоговую службу, Отделение Социального фонда России, государственному учреждению и Территориальному Фонду обязательного медицинского страхования, а также иному уполномоченному органу допускается по основаниям, предусмотренным законодательством Российской Федерации.

8.6.3. Раскрытие персональных данных третьему лицу без согласия соответствующего субъекта не допускается, за исключением случаев, когда это необходимо для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных.

8.6.4. Трансграничная передача персональных данных на территории иностранных государств не осуществляется.

8.7. Распространение персональных данных:

8.7.1. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с учетом выполнения требований, предусмотренных законодательством Российской Федерации о персональных данных.

8.7.2. В случае если субъект сам раскрывает свои персональные данные неопределенному кругу лиц при помощи функционала Интернет-сайта или сервиса Учреждения без предоставления соответствующего согласия, дальнейшее распространение другими операторами персональных данных возможно только на основании согласия соответствующего субъекта на обработку персональных данных, разрешенных для распространения.

8.7.3. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

8.8. Условия и порядок прекращения обработки персональных данных:

8.8.1. Учреждение прекращает обработку персональных данных в следующих случаях:

- достигнута цель их обработки.
- истек срок действия или отозвано согласие субъекта персональных данных на обработку указанных данных, когда по Закону о персональных данных обработка этих данных допускается только с согласия.
- выявлен факт их неправомерной обработки. Срок - в течение трех рабочих дней с даты выявления.

8.8.2. В случае достижения цели обработки персональных данных обработка таких персональных данных должна быть прекращена, а персональные данные должны быть уничтожены в 30-дневный срок с даты достижения цели обработки персональных данных.

8.8.3. В случае отзыва субъектом согласия на обработку его персональных данных обработка таких персональных данных должна быть прекращена, и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, такие персональные данные подлежат уничтожению в течение 30 (тридцати) дней с даты поступления указанного отзыва.

8.8.4. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку Учреждение прекращает обработку этих данных, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных,
- Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации,
- иное не предусмотрено другим соглашением между Учреждением как Оператором и субъектом ПД.

8.8.5. При обращении субъекта персональных данных с требованием о прекращении обработки персональных данных в срок, не превышающий 10 рабочих дней с даты получения Учреждением соответствующего требования, обработка персональных данных прекращается, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Учреждение направляет субъекту ПД мотивированное уведомление с указанием причин продления срока.

8.8.6. В случае выявления неправомерной обработки персональных данных, в том числе при обращении субъекта ПД или его представителя, либо по запросу субъекта ПД или его представителя, либо Роскомнадзора, обработка таких персональных данных должна быть прекращена в течение 3 (трех) рабочих дней либо блокирована на период проверки. Если обеспечить правомерность обработки персональных данных невозможно, персональные данные подлежат уничтожению в течение 10 (десяти) рабочих дней с даты выявления неправомерной обработки.

Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос Роскомнадзора были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

8.9. Хранение персональных данных:

8.9.1. 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 законодательством Российской Федерации либо договором, стороной которого является субъект персональных данных.

8.9.2. Хранение персональных данных осуществляется с учетом обеспечения режима их конфиденциальности.

8.9.3. Персональные данные передаются на архивное хранение в соответствии с законодательством Российской Федерации об архивном деле, уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в

достижении этих целей, если иное не предусмотрено законодательством Российской Федерации либо договором, стороной которого является субъект персональных данных.

8.10. Порядок уничтожения персональных данных:

8.10.1. Условия и сроки уничтожения персональных данных:

- достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;
- достижение максимальных сроков хранения документов, содержащих персональные данные, - в течение 30 дней;
- предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - в течение 7 (семи) рабочих дней;
- отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

8.10.2. Уничтожение персональных данных осуществляет комиссия, созданная приказом главного врача Учреждения.

8.10.3. Способы уничтожения персональных данных устанавливаются в локальных нормативных актах Учреждения.

8.10.4. В случае отсутствия возможности уничтожения персональных данных в течение указанных выше сроков, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает их уничтожение в срок не более 6 (шести) месяцев, если иной срок не установлен законодательством Российской Федерации.

8.11. Актуализация, исправление и удаление персональных данных:

8.11.1. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение обязано внести в них необходимые изменения.

8.11.2. Учреждение обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

8.11.3. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Учреждение обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование с момента такого обращения/получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

8.11.4. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение в течение 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

8.11.5. При выявлении Учреждением, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Учреждение:

✓ в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятым мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;

✓ в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

9. Сроки обработки и хранения персональных данных

9.1. Сроки обработки персональных данных ограничиваются достижением заявленной цели и напрямую зависят от сроков хранения трудовых договоров и документов кадрового и бухгалтерского учета, гражданско-правовых договоров и медицинской документации и составляют:

9.1.1. Срок хранения персональных данных работников составляет 50/75 лет ЭПК с момента прекращения трудовых отношений с работником. Уничтожение персональных данных осуществляется в установленные законодательством сроки по истечению периода их хранения либо при наступлении иных законных оснований.

9.1.2. Срок хранения персональных данных претендентов, включенных в кадровый резерв, составляет 5 лет (в случае включения в кадровый резерв) с момента принятия соответствующего решения. Уничтожение персональных данных осуществляется в установленные законодательством сроки по истечению периода их хранения, при поступлении отзыва согласия субъекта либо при наступлении иных законных оснований.

9.1.3. Срок хранения персональных данных соответствует сроку хранения первичных медицинских документов (медицинской карты) и составляет 25 лет (для детей – 10 лет) в Учреждении, 75 лет – в архиве.

Основанием для обработки персональных данных является Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Договор; Согласие субъекта. Согласие может быть отозвано путем подачи письменного заявления. Уничтожение персональных данных осуществляется в установленные законодательством сроки по истечению периода их хранения либо при наступлении иных законных оснований.

9.1.4. Срок обработки персональных данных контрагентов и прочих клиентов Учреждения (физических лиц), в том числе полученных в связи с заключением договора на оказание медицинских услуг, составляет 5 лет с момента оформления первичного учетного документа. Уничтожение персональных данных осуществляется в установленные законодательством сроки по истечению периода их хранения либо при наступлении иных законных оснований.

9.2. Персональные данные на бумажных носителях хранятся в Учреждении в течение сроков хранения документов, для которых эти сроки предусмотрены трудовым законодательством, законодательством в сфере охраны здоровья граждан, законодательством об архивном деле в РФ и др.

9.3. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

9.4. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

9.5. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

10. Порядок предоставления информации и взаимодействия с субъектом персональных данных.

10.1. Субъект персональных данных 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 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 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 Федеральным законом «О персональных данных» или другими федеральными законами.

10.2. Указанные выше сведения должны быть предоставлены субъекту ПД Учреждением 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.

10.3. Сведения, указанные в пункте 10.1, предоставляются субъекту ПД или его представителю Учреждением при обращении либо при получении запроса субъекта ПД или его представителя.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе,
- сведения, подтверждающие участие субъекта ПД в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением,
- подпись субъекта ПД или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются субъекту ПД или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Если в обращении (запросе) субъекта ПД не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Право субъекта ПД на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта ПД к его персональным данным нарушает права и законные интересы третьих лиц.

10.4. В случае если сведения, указанные в пункте 10.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Учреждение или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.1, и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения/запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект ПД вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 10.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения указанного срока, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 10.1, должен содержать обоснование направления повторного запроса.

Учреждение вправе отказать субъекту ПД в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 10.4 и 10.5. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

10.5. Учреждение обязано сообщить субъекту ПД или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту ПД, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта ПД или его представителя либо в течение 30 дней с даты получения запроса субъекта ПД или его представителя.

10.6. Учреждение обязано предоставить безвозмездно субъекту ПД или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту ПД.

11. Организация обработки и защиты персональных данных

11.1. Организация обработки персональных данных осуществляется в Учреждении в следующем порядке:

- назначение ответственных лиц за организацию обработки персональных данных,
- установление Перечня лиц, имеющих доступ к персональным данным,
- утверждение настоящей Политики и иных локальных актов по вопросам обработки персональных данных,
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных,
- осуществление внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Учреждения,
- осуществление оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определение соотношения указанного вреда и принимаемых Учреждением как Оператором персональных данных мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом,
- ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политикой, локальными актами по вопросам обработки персональных данных, и/или обучение указанных работников.

11.2. Учреждение при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

- ✓ определяет угрозы безопасности персональных данных при их обработке, в том числе в информационных системах персональных данных;
- ✓ принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
- ✓ назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;
- ✓ создает необходимые условия для работы с персональными данными;
- ✓ организует учет документов, содержащих персональные данные;
- ✓ организует работу с информационными системами, в которых обрабатываются персональные данные;
- ✓ хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;
- ✓ организует обучение работников Оператора, осуществляющих обработку персональных данных;
- ✓ применяет организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- ✓ применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;

- ✓ оценивает эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- ✓ учитывает машинные носители персональных данных;
- ✓ обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;
- ✓ восстанавливает персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
- ✓ осуществляет регистрацию и учет действий, совершаемых с персональными данными в информационных системах и базах данных;
- ✓ устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- ✓ осуществляет контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

12. Порядок обработки персональных данных в информационных системах

12.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

12.2. Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах Учреждения, осуществляется в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

12.3. Работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника либо в соответствии с обязанностями, возложенными на него соответствующим локальным актом Учреждения (приказом, распоряжением).

12.4. Информация может вноситься как в автоматическом режиме при получении персональных данных из других систем (например, Федеральный регистр медицинских работников), так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

12.5. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах Учреждения, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками (работниками, ответственными за организацию обработки персональных данных и за информационную безопасность, работниками отдела АСУ) незамедлительно принимаются меры по установлению причин нарушений и их устранению.

12.6. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

12.7. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются

персональные данные;

- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации и технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

12.8. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

✓ Угрозы первого типа актуальны для информационной системы, если для нее, в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

✓ Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

✓ Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

12.9. В соответствии с пунктом 11 статьи 19 Федерального закона «О персональных данных» под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

При обработке персональных данных в информационных системах (далее – ИС) устанавливаются четыре уровня защищенности персональных данных.

12.9.1. Необходимость обеспечения первого уровня защищенности персональных данных при их обработке в ИС устанавливается при наличии хотя бы одного из следующих условий:

а) для ИС актуальны угрозы первого типа и ИС обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы ИС актуальны угрозы второго типа и ИС обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Учреждения.

12.9.2. Необходимость обеспечения второго уровня защищенности персональных данных при их обработке в ИС устанавливается при наличии хотя бы одного из следующих условий:

а) для ИС актуальны угрозы первого типа и ИС обрабатывает общедоступные персональные данные;

б) для ИС актуальны угрозы второго типа и ИС обрабатывает специальные категории персональных данных сотрудников Учреждения или специальные категории персональных

данных менее чем 100 000 субъектов ПД, не являющихся сотрудниками Учреждения;

в) для ИС актуальны угрозы второго типа и ИС обрабатывает биометрические персональные данные;

г) для ИС актуальны угрозы второго типа и ИС обрабатывает общедоступные персональные данные более чем 100000 субъектов ПД, не являющихся сотрудниками Учреждения;

д) для ИС актуальны угрозы второго типа и ИС обрабатывает иные категории персональных данных более чем 100000 субъектов ПД, не являющихся сотрудниками Учреждения;

е) для ИС актуальны угрозы третьего типа и ИС обрабатывает специальные категории персональных данных более чем 100000 субъектов ПД, не являющихся сотрудниками Учреждения.

12.9.3. Необходимость обеспечения третьего уровня защищенности персональных данных при их обработке в ИС устанавливается при наличии хотя бы одного из следующих условий:

а) для ИС актуальны угрозы второго типа и ИС обрабатывает общедоступные персональные данные сотрудников Учреждения или общедоступные персональные данные менее чем 100000 субъектов ПД, не являющихся сотрудниками Учреждения;

б) для ИС актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных сотрудников Учреждения или иные категории персональных данных менее чем 100 000 субъектов ПД, не являющихся сотрудниками Учреждения;

в) для ИС актуальны угрозы третьего типа и ИС обрабатывает специальные категории персональных данных сотрудников Учреждения или специальные категории персональных данных менее чем 100000 субъектов ПД, не являющихся сотрудниками Учреждения;

г) для ИС актуальны угрозы третьего типа и ИС обрабатывает биометрические персональные данные;

д) для ИС актуальны угрозы третьего типа и ИС обрабатывает иные категории персональных данных более чем 100000 субъектов ПД, не являющихся сотрудниками Учреждения.

12.9.4. Необходимость обеспечения четвертого уровня защищенности персональных данных при их обработке в ИС устанавливается при наличии хотя бы одного из следующих условий:

а) для ИС актуальны угрозы третьего типа и ИС обрабатывает общедоступные персональные данные;

б) для ИС актуальны угрозы третьего типа и ИС обрабатывает иные категории персональных данных сотрудников Учреждения или иные категории персональных данных менее чем 100000 субъектов ПД, не являющихся сотрудниками Учреждения.

12.10. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

13. Ответственность

13.1. Контроль за исполнением требований настоящей Политики осуществляется лицами, назначенными приказом главного врача ответственными за организацию обработки персональных данных.

13.2. Ответственность за нарушение Учреждением требований законодательства Российской Федерации и нормативных актов в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

13.3. За нарушение требований, установленных законодательством Российской Федерации, настоящей Политикой, Положением об обработке и защите персональных данных и другими локальными актами Учреждения, работники и иные лица, получившие доступ к персональным данным, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с Федеральными законами Российской Федерации.

14. Заключительные положения

14.1. Настоящая Политика вступает в силу с момента ее утверждения главным врачом и действует бессрочно, до замены ее новой Политикой.

14.2. Учреждение имеет право вносить изменения в настоящую Политику.

14.3. В случае если отдельные положения настоящей Политики войдут в противоречие с действующим законодательством Российской Федерации в сфере обработки и защиты персональных данных, применяются положения действующего законодательства.

14.4. Действующая редакция хранится в месте нахождения Учреждения по адресу: 600009, г. Владимир, ул. Каманина, д. 25, здание административного корпуса.