

Политика
обработки персональных данных
БУ «Окружной кардиологический диспансер
«Центр диагностики и сердечно-сосудистой хирургии»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика обработки персональных данных (далее – Политика):

- является основополагающим внутренним документом БУ «Окружной кардиологический диспансер «Центр диагностики и сердечно-сосудистой хирургии» (далее – Учреждение), регулирующим вопросы обработки персональных данных (далее – ПДн);
- разработана в целях обеспечения соответствия законодательству Российской Федерации обработки, хранения и защиты персональных данных сотрудников и граждан;
- раскрывает основные категории персональных данных, обрабатываемых Учреждением, цели, способы и принципы обработки персональных данных, права и обязанности Учреждения при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Учреждением в целях обеспечения безопасности персональных данных при их обработке;
- предназначена для сотрудников Учреждения, осуществляющих обработку персональных данных в целях непосредственной реализации ими закрепленных в Политике принципов, а также является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Учреждения при обработке персональных данных;
- подлежит публикации в сети Интернет на официальном сайте БУ «Окружной кардиологический диспансер «Центр диагностики и сердечно-сосудистой хирургии».

**2. ИСТОЧНИКИ НОРМАТИВНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ ВОПРОСОВ ОБРАБОТКИ
ПЕРСОНАЛЬНЫХ ДАННЫХ**

Политика Учреждения в области обработки персональных данных определяется на основании следующих нормативных правовых актов Российской Федерации:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Уголовный кодекс Российской Федерации;

- Указ Президента Российской Федерации от 06.03.1997г. №188 «Об утверждении перечня сведений конфиденциального характера»;
- Федеральный закон от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687;
- Т к защите персональных данных при их обработке в информационных системах персональных данных, утверждены Постановлением Правительства Российской Федерации от 01.11.2012 г. №1119;
- нормативные и методические документы ФСБ России, ФСТЭК России, Роскомнадзора.

3. ОСНОВНЫЕ ТЕРМИНЫ И ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В ЛОКАЛЬНЫХ ДОКУМЕНТАХ УЧРЕЖДЕНИЯ, ПРИНИМАЕМЫХ ПО ВОПРОСУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

АРМ – автоматизированное рабочее место. программно-технический комплекс, предназначенный для автоматизации деятельности в Учреждении.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных (далее – ПДн), в том числе их передачи.

Врачебная тайна – это не подлежащие разглашению сведения о пациенте, факте обращения за медицинской помощью, диагнозе и иные сведения о состоянии здоровья и частной жизни, полученные в результате обследования и лечения.

Доступ к информации – возможность получения информации и ее использования.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Информация – сведения (сообщения, данные) независимо от формы их представления (в соответствии с Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информатизации и защите информации").

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

Информационная система персональных данных (далее – ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором персональных данных или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.

Криптографическое средство защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Пациент – физическое лицо, обратившееся за медицинской помощью, получающее медицинскую помощь и связанные с ней услуги независимо от наличия или отсутствия у него заболевания.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Персональные данные работников Учреждения – информация, которая необходима работодателю в связи с трудовыми отношениями и касается конкретного работника.

Персональные данные пациентов Учреждения – информация, которая необходима Учреждению для оказания медицинской помощи пациенту и связанных с ней услуг.

Правовая защита информации – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

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

Работник – физическое лицо, состоящее в трудовых отношениях с Учреждением.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

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

Сертификация на соответствие требованиям по безопасности информации – форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Специальные категории персональных данных – сведения о субъекте персональных данных, касающиеся его национальной принадлежности, состояния здоровья, интимной жизни.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации

Субъект персональных данных – физическое лицо, которому принадлежат персональные данные.

Техническая защита информации – Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей

(подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты. К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

4. ОБЩИЕ УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка ПДн в Учреждении осуществляется на основе следующих принципов:

4.1.1. Законность и справедливости обработки ПДн.

4.1.2. Законность целей и способов обработки ПДн и добросовестности.

4.1.3. Соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Учреждения.

4.1.4. Соответствие содержания и объема обрабатываемых ПДн целям обработки ПДн.

4.1.5. Достоверность ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн.

4.1.6. Недопустимость объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.7. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.8. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом «О персональных данных».

4.1.9. Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Учреждению своих ПДн.

4.1.10. Держателем ПДн является Учреждение, которому субъект ПДн передает во владение свои ПДн. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

4.1.11. Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн и обеспечивает безопасность информации в процессе деятельности Учреждения.

4.1.12. Учреждение при обработке ПДн обязан принимать необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн.

4.1.13. Мероприятия по защите ПДн определяются приказом «О защите конфиденциальной информации в бюджетном учреждении ХМАО – Югры «Окружной кардиологический диспансер «Центр диагностики и сердечно-сосудистой хирургии», а также приказами, инструкциями и другими внутренними документами Учреждения.

4.2. Для защиты ПДн в Учреждении применяются следующие правила:

4.2.1. Ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн;

4.2.2. Строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

4.2.3. Знание сотрудниками требований нормативно-методических документов по защите ПДн;

4.2.4. Распределение персональной ответственности между сотрудниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн;

4.2.5. Установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных;

4.2.6. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

4.2.7. Исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка ПДн и находится соответствующая вычислительная техника;

4.2.8. Организация порядка уничтожения персональных данных;

4.2.9. Своевременное выявление нарушений требований разрешительной системы доступа;

4.2.10. Регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн;

4.2.11. Ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн;

4.2.12. Создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией;

4.2.13. Резервирование защищаемых данных (создание резервных копий).

4.3. Цели обработки персональных данных:

4.3.1. Соблюдение требований трудового законодательства Российской Федерации;

4.3.2. Оказание медицинских и медико-социальных услуг, установление медицинского диагноза.