Бюджетное учреждение Ханты-Мансийского автономного округа
«ПИОНЕРСКАЯ РАЙОННАЯ БОЛЬНИЦА»
(БУ «Пионерская районная больница)

П Р И К А З

Об утверждении политики обработки и защиты персональных данных
БУ «Пионерская районная больница»

«02» 03 2021 г. № 145

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением правительства Российской Федерации от 01.11.20123 № 1119 «Об утверждении требований о защите персональных данных при обработке в информационных системах персональных данных»,-

п р и к а з ы в а ю:

1. Утвердить «Политику обработки и защиты персональных данных бюджетного учреждения Ханты-Мансийского автономного округа-Югры «Пионерская районная больница» (далее-Политика) (Приложение).

2. Заместителям руководителя, заведующим отделениями, главной медицинской сестре, старшим медицинским сестрам и начальникам отделов:

2.1. ознакомить работников подведомственных подразделений с Политикой под подпись;

3. Бадышевой Т.Н.-юрисконсульту ОП и КР:

3.1. Сформировать папку по внутренней электронной сети:

- в папках «Стационар», «Поликлиника», «Замы» - папку «Политика информационной безопасности 2021» (для ознакомления работников учреждения и для осуществления внутреннего контроля над исполнением требований Политики).

4. Контроль за исполнения настоящего приказа оставляю за собой.

Главный врач Берднидцкая М.Е.

Политика
обработки и защиты персональных данных
бюджетного учреждения Ханты-Мансийского автономного округа-Югры
«Пионерская районная больница»

1.Общие положения

1.1. Настоящая политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с п. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных № (далее – Закон о ПДн) и является основополагающим внутренним регулятивным документом бюджетного учреждения Ханты-Мансийского автономного –округа-Югры «Пионерская районная больница» (далее Учреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее- ПДн), оператором которых является - Учреждение.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в Учреждении осуществляется в связи с выполнением Учреждений функций, предусмотренных её учредительными документами, и определяемых:

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

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

- Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральным законом от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи»;

-Трудовым кодексом Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ, ст. 85-90);

- Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональной данных при обработке в информационных системах персональных данных»;

- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ним отношений, в которых Учреждение выступает в качестве работодателя (гл. 14 Трудового кодекса российской Федерации), в связи с реализацией Учреждением своих прав и обязанностей как юридического лица.

1.5. ПДн получаются и обрабатываются Учреждением на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

1.6. В целях исполнения возложенных на Учреждение функций Учреждение в установленном порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Учреждение поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные законодательством требования к обработке и защите ПДн.

1.7. Учреждение предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

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

1.9. Действующая редакция хранится на месте нахождения Учреждения по адресу: пгт. Пионерский, ул. Советский, 65; электронная версия Политики – на сайте по адресу: pionerbol-adm@yandex.ru.

2. Термины и определения

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- адрес;
- семейное положение;
- социальное положение;
- имущественное положение;
- сведения об образовании;
- сведения о профессии;
- сведения о доходах;
- сведения о состоянии здоровья

другая информация.

Защищаемая информация – информация, подлежащая защите в соответствии с требованиями нормативных документов в области безопасности информации или требованиями, установленными собственником информации.

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или неопределённому 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.

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

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

Нарушитель безопасности - физической лицо, случайно или преднамеренно совершающие действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах.

Угроза безопасности информации - некая совокупность факторов и условий, которая создает опасность в отношении защищаемой информации.

Правила разграничения доступа – совокупность правил, регламентирующих порядок и условия доступа субъектов доступа (сотрудников, программ) к объектам доступа (информации, её носителям, процессам и другим ресурсам).

Несанкционированный доступ (несанкционированные действия, НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационным системам.

Контролируемая зона – это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Дополнительные устройства обмена информацией – портативные жесткие диски, съемные флэш – носители, CD, DVD – диски.

Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемиологических (профилактических) мероприятий.

Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3. Принципы обеспечения безопасности персональных данных.

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Учреждении является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Учреждение руководствуются следующими принципами:

- законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

- системность: обработка ПДн в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

- комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения (далее – ИС) и других имеющихся в Учреждении систем и средств защиты;

- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Учреждения (далее – ИСПДн), а также объема и состава обрабатываемых ПДн;

- открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Учреждения (далее - СЗПДн) не дают возможности преодоления имеющихся в учреждении систем защиты возможными нарушителями безопасности ПДн;

- научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатации СЗПДн осуществляется Работниками, имеющими необходимые для этого квалификацию и опыт;

- эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Учреждения предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

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

- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются;

3.3. В учреждении не производится обработка ПДН, несовместимая с целями их сбора.

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

4. Обработка персональных данных

4.1. Получение персональных данных.

4.1.1.Все персональные данные следует получать от самого субъекта. Если ПДн субъекта можно получить у третей стороны, то субъект должен уведомлен об этом или от него должно получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течении которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПДн создаются путем:

- копирование оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное удостоверение и др.);
- внесение сведений в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.);

Порядок доступа субъекта ПДн к его ПДн, обрабатываемом Учреждением, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Учреждения.

4.2. Обработка персональных данных.

4.2.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения, возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

Доступ работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

Допущенные к обработке ПДн работники под роспись знакомятся с документами учреждения, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников.

Учреждением производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

4.2.2. Цели обработки ПДн:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 г. № 61 –ФЗ «Об обращении лекарственных средств», от 29.11.2010 года № 326 – ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утверждёнными Постановлением Правительства российской Федерации от 04.10.2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений;

4.2.3. Категория субъектов персональных данных

В учреждении обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющие близкими родственниками сотрудников учреждения;

- физические лица, уволившиеся с учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

4.2.4. Персональные данные обрабатываемые Учреждением:
- данные полученные при осуществлении трудовых отношений;
- данные полученные при осуществлении отбора кандидатов на работу в учреждение;
-данные полученные при осуществлении гражданско-правовых отношений;
- данные полученные при оказании медицинской помощи.

4.2.5. Обработка персональных данных ведётся:
- с использованием средств автоматизации;
- без использования средств автоматизации;

4.3. Хранение персональных данных

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

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

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

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

4.3.5. Хранение ПДн в форме, позволяющей определить субъекта в ПДн, осуществляется на дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение персональных данных

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

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

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

4.5. Передача персональных данных

4.5.1. Учреждение передает ПДн третьим лицам в следующих случаях:
- субъект отразил свое согласие на такие действия;
-передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым передаются персональные данные

Третьи лица, которым передаются персональные данные:
- пенсионный фонд Российской Федерации (на законных основаниях);
- налоговые органы Российской Федерации (на законных основаниях);
- фонд социального страхования (на законных основаниях);- территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);

- судебные и правоохранительные органы в случаях, установленных законодательством;

- бюро кредитных историй (с согласия субъекта);

- юридические фирмы, работающие в рамках законодательства Российской Федерации, при неисполнения обязательств по договору займа (с согласия субъекта).

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов учреждения создана система защиты персональных данных (СЗПДн), состоящая из подсистем правовой организационной и технической защиты.

5.2. Подсистема правовой защиты представляет комплекс правовой организационно-распорядительных и нормативных документов, обеспечивающие создание функционирования и совершенствования СЗПДн.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

Основными мерами защиты персональных данных, используемыми учреждением являются:

-назначение лица ответственного за обработку персональных данных, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;

- определение актуальных угроз безопасности ПДн при обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;

- разработка политики в отношении обработки персональных данных;

- установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПД;

- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

- применение прошедших подготовку в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности;

- сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

- сертифицированное программное средство защиты информации от несанкционированного доступа;

- обучение работников учреждения непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику учреждения в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

- осуществление внутреннего контроля и аудита.

6.Основные права субъекта персональных данных и обязанности учреждения

6.1.Основные права субъекта персональных данных

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 оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 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 настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн вправе требовать от оператора 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.

6.2. Обязанности учреждения

Учреждение обязано:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
-опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
-принимать необходимые правовые, организационные и технические меры или обеспечивать их принятые для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.