

УТВЕРЖДАЮ
Главный врач КГБУЗ
«Хабаровская районная больница»
министерства здравоохранения
Хабаровского края
Ю.В. Маленьких
«__» _____ 20__ г.

Политика информационной безопасности ИСПДн КГБУЗ «Хабаровская районная больница»

Введение

Настоящая Политика Краевого государственного бюджетного учреждения здравоохранения «Хабаровская районная больница» министерства здравоохранения Хабаровского края (далее – КГБУЗ «Хабаровская районная больница») в отношении обработки персональных данных (далее – Политика) разработана в соответствии с требованиями нормативно-правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой персональных данных (далее – ПДн).

Политика определяет принципы сбора, обработки, хранения, передачи защиты ПДн физических лиц (далее субъекты ПДн), реализуемые в КГБУЗ «Хабаровская районная больница» (далее – Оператор).

Действие настоящей Политики распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПДн, осуществляемых как с использованием средств автоматизации, так и без использования таких средств.

В рамках реализации настоящей Политики Оператором разработаны другие внутренние нормативные документы, регламентирующие отдельные процессы обработки и защиты ПДн.

1. Нормативная документация

Настоящая Политика разработана с учетом требований следующих документов:

- Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон Российской Федерации от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Трудовой кодекс Российской Федерации;
- Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1. Общие положения

1.1. Оператор осуществляет обработку ПДн следующих категорий субъектов ПДн:

- работники Оператора;
- субъекты ПДн (пациенты, для учета медицинских услуг);
- заявители (для рассмотрения обращений);
- медицинские работники учреждений здравоохранения Хабаровского края (оказывающие медицинские услуги).

1.2. Оператор осуществляет обработку ПДн, руководствуясь следующими принципами:

- обработка ПДн осуществляется в соответствии с действующим законодательством РФ;
- обработка ПДн осуществляется для достижения конкретных, заранее определенных целей; обработка ПДн, не оправданная достижением таких целей, не осуществляется;
- ПДн, цели обработки которых не совместимы, не объединяются;
- содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки;
- при обработке ПДн обеспечивается их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям их обработки;
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн;
- ПДн уничтожаются или обезличиваются при достижении целей их обработки, утрате необходимости в достижении этих целей или окончании срока хранения ПДн, определенного, согласием на обработку ПДн, федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

1.3. В целях обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами Оператор:

- назначает ответственного за организацию обработки ПДн;
- утверждает внутренние нормативные и распорядительные документы по вопросам обработки ПДн, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применяет правовые, организационные и технические меры по обеспечению безопасности ПДн;
- осуществляет внутренний контроль соответствия обработки ПДн требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», принятых в соответствии с ним нормативных правовых актов, внутренних нормативных и распорядительных документов Оператора, регулирующих обработку ПДн;
- проводит оценку вреда, который может быть причинен субъектам ПДн в случае нарушения Оператором требований законодательства в области ПДн, соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения своих обязанностей, предусмотренных законодательством в области ПДн;
- ознакомливает своих работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации в области ПДн, в том числе с требованиями к защите ПДн, внутренними нормативными и распорядительными документами Оператора, регулирующими обработку ПДн.
- публикует настоящую Политику на официальном сайте Оператора, обеспечивая беспрепятственный доступ к ней неограниченного круга лиц.

2. Получение, обработка и защита персональных данных

2.1. Порядок получения персональных данных.

- Оператор по возможности получает все обрабатываемые им ПДн непосредственно у субъектов ПДн. В случаях, когда получение ПДн непосредственно у субъектов ПДн невозможно, Оператор предпринимает предусмотренные действующим законодательством меры по соблюдению прав субъектов ПДн при получении их ПДн от третьих лиц.
- В случаях, когда действующим законодательством требуется получение согласия субъекта ПДн на обработку его ПДн, Оператор обрабатывает его ПДн только при наличии такого согласия и с соблюдением ограничений на объем, сроки и способы обработки ПДн, предусмотренных таким согласием.

- Оператор не получает и не обрабатывает ПДн субъекта ПДн о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности.
- Оператор предоставляет своим работникам доступ к минимальному объему ПДн, необходимому им для выполнения своих служебных обязанностей.
- Работники Оператора допускаются к обработке ПДн только после ознакомления с требованиями действующего законодательства и внутренних нормативных и распорядительных документов Оператора, регулирующих обработку и защиту ПДн, и подписания обязательства о неразглашении конфиденциальной информации.

2.2. Порядок обработки персональных данных.

- Обработка ПДн осуществляется Оператором только в целях, заявленных при их сборе (получении). В частности, обработка ПДн сотрудников осуществляется в целях исполнения возложенных на Оператора действующим законодательством и трудовым договором обязанностей работодателя, а обработка ПДн пациентов, заявителей в целях оказания медицинских, государственных услуг и рассмотрения обращений.
- При определении объема и содержания, обрабатываемых ПДн, Оператор руководствуется Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и иными федеральными законами в области защиты ПДн, а также принципом соответствия объема и содержания обрабатываемых ПДн заявленным целям их обработки.
- При принятии решений, затрагивающих интересы субъекта ПДн, Оператор не имеет права основываться на результатах исключительно автоматизированной обработки его ПДн, кроме случаев, наличия согласия в письменной форме субъекта ПДн на принятие таких решений и случаев, предусмотренных федеральными законами.

2.3. Порядок защиты персональных данных.

- Защита ПДн субъекта ПДн от неправомерного их использования или утраты обеспечивается Оператором за счет его средств в порядке, установленном федеральными законами Российской Федерации в области защиты ПДн.
- Оператор принимает необходимые организационные и технические меры для защиты ПДн от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.
- Оператор привлекает к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту ПДн субъекта ПДн.
- Оператор исключает доступ к ПДн субъектов ПДн своих работников, не включенных в Перечень лиц, допущенных к обработке ПДн.
- Копировать и делать выписки ПДн субъектов ПДн сотрудникам Оператора разрешается исключительно в служебных целях.
- Сохранение и защита ПДн субъектов ПДн осуществляются Оператором в соответствии с требованиями действующего законодательства независимо от наличия соответствующих требований со стороны субъектов ПДн.

3. Хранение персональных данных

- Оператор осуществляет учет всех хранимых им ПДн, независимо от формы их представления.
- ПДн на бумажных носителях хранятся Оператором в специально оборудованных помещениях, шкафах и сейфах, которые запираются.
- В процессе хранения ПДн субъектов ПДн Оператор осуществляет контроль достоверности и полноты ПДн, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4. Передача персональных данных

Оператор передает находящиеся в его распоряжении ПДн третьим лицам в следующих случаях:

- При наличии письменного согласия субъекта ПДн на передачу его ПДн третьему лицу, включающего наименование или фамилию, имя, отчество и адрес третьего лица, цели, сроки и способы обработки третьим лицом ПДн.
- В случае если передача ПДн третьему лицу необходима для выполнения обязательств Оператора перед субъектом ПДн.

- В случае если обязанность по передаче ПДн третьему лицу возложена на Оператора действующим законодательством.

5. Уничтожение персональных данных

- Уничтожение ПДн производится Оператором в случаях и в порядке, предусмотренных действующими законами и принятыми в соответствии с ними нормативными правовыми актами.
- При уничтожении ПДн как на бумажных, так и на электронных носителях Оператор обеспечивает невозможность их последующего восстановления.

6. Права субъекта ПДн

- Субъект ПДн вправе требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
- Субъект ПДн имеет право на получение от Оператора информации, касающейся обработки его ПДн, в том числе содержащей:
 - правовые основания и цели обработки ПДн;
 - применяемые Оператором способы обработки ПДн;
 - наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании Федерального закона;
 - обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения;
 - сроки обработки ПДн, в том числе сроки их хранения;
 - порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
 - информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
 - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
 - иные сведения, предусмотренные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.
- Субъект ПДн имеет право требовать исключить или исправить неверные, или неполные ПДн, а также ПДн, обрабатываемые с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Субъект ПДн имеет право на обжалование в судебном порядке любых неправомерных действий или бездействия Оператора при обработке и защите его ПДн.