УТВЕРЖДАЮ

Главный врач ГБУЗ «Кузнецкая межрайонная больница»

_____ А.В. Потапов

/____ /_____/ 2016 г.

Государственное бюджетное учреждение здравоохранения «Кузнецкая межрайонная больница»

Защита персональных данных

ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

_____ №_____

Листов 13

2016

СОДЕРЖАНИЕ

1. Область применения

Действие документа (далее - Политика) распространяется на процессы Государственного бюджетного учреждения здравоохранения «Кузнецкая межрайонная больница» (далее - Учреждение), в которых осуществляется обработка персональных данных субъектов персональных данных всех категорий, а также на подразделения, принимающие участие в вышеуказанных процессах.

Основные положения документа могут быть распространены также на подразделения других организаций, осуществляющие взаимодействие с Учреждением в качестве поставщиков и потребителей (пользователей) информации.

2. Назначение

Настоящая Политика определяет политику Учреждения в отношении обработки персональных данных (далее – ПДн).

Настоящая Политика составлена в соответствии с п. 2 ст. 18.1 ФЗ-152 «О персональных данных» и действует в отношении всех ПДн, обрабатываемых в Учреждении, которые могут быть получены от субъекта ПДн, являющегося стороной по гражданско-правовому договору с Учреждением (далее - Клиента), или от субъекта ПДн, состоящего с Учреждением в отношениях, регулируемых трудовым законодательством (далее - Работника).

Учреждение обязуется опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.

Целью настоящей Политики является защита интересов Учреждения, ее клиентов, партнеров и работников, а также выполнение требований Законодательства Российской Федерации в области обработки и защиты ПДн.

Политика распространяется на ПДн, полученные как до, так и после утверждения настоящей Политики.

3. Термины и определения

В настоящем документе применены следующие термины с соответствующими определениями:

доверенная среда эксплуатации ИСПДн: среда, в которой обеспечение необходимого уровня безопасности персональных данных, гарантируется выполнением требований разрешительных документов уполномоченных федеральных органов, включая ФСБ России и (или) ФСТЭК России.

доверенный канал: средство взаимодействия между функциями безопасности объекта и удаленным доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании политики безопасности объекта.

доверие: основание для уверенности в том, что сущность отвечает своим целям безопасности.

информационная система: совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

информационная система персональных данных: 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.

информационные технологии: процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

линии связи: линии передачи, физические цепи и линейно-кабельные сооружения связи.

нарушитель безопасности персональных данных: физическое лицо случайно или преднамеренно совершающее действия, следствием которых является нарушение заданных характеристик безопасности персональных данных при их обработке в информационной системе персональных данных.

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.

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.

система защиты персональных данных: совокупность организационных мер и средств защиты информации, включающих средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в информационной системе информационные технологии.

оператор: государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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;

4. Обозначения и сокращения

В настоящем документе применены следующие обозначения и сокращения:

ИСПДн – информационная система персональных данных

ИТ–инфраструктура – информационно-технологическая инфраструктура

МРМ – мобильное рабочее место

НСД – несанкционированный доступ

ПДн – персональные данные

ПТК – программно-технический комплекс

СЗПДн – система защиты персональных данных

СКЗИ – средство криптографической защиты информации

УБПДн – угрозы безопасности персональных данных

5. Правовые основы обеспечения безопасности персональных данных

Политика разработана в целях реализации требований Федерального закона № 152-ФЗ от 27.07.2006 года «О персональных данных» по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Учреждения и выполнения международных обязательств РФ.

Правовую основу Политики составляют Конституция Российской Федерации, Концепция национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации, Федеральные законы РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ, нормативные правовые акты (приказы, распоряжения) федеральных органов исполнительной власти, уполномоченных в обеспечении безопасности и технической защиты информации (ЗИ), а также международные договоры РФ.

6. Принципы обработки персональных данных

Обработка ПДн в Учреждении осуществляется в соответствии с принципами, установленными Федеральным законом РФ «О персональных данных»:

– обработка ПДн осуществляется на законной и справедливой основе;

– обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;

– не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместных между собой;

– обработке подлежат только те ПДн, которые отвечают целям их обработки;

– содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточными по отношению к заявленным целям обработки;

– при обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки. Оператор принимает необходимые меры и обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

– хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн. 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.

7. Цели сбора и обработки персональных данных

Учреждение собирает и хранит ПДн клиентов и работников, необходимые для оказания услуг, исполнения соглашения и договора, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

Учреждение может использовать ПДн в следующих целях:

– идентификация стороны в рамках договоров Учреждения;

– связь с Клиентом в случае необходимости, в том числе направление уведомлений, информации и запросов, связанных с оказанием услуг, а также обработка заявлений, запросов, платежных поручений и заявок Клиента;

– улучшение качества услуг, оказываемых Учреждением;

– продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с Клиентом;

– учреждение собирает и хранит ПДн работника, необходимые для исполнения условий трудового договора и осуществления прав и обязанностей в соответствии с трудовым законодательством;

– учреждение собирает и хранит ПДн работника, необходимые для заключения и ведения договоров медицинского страхования, организации выплат заработанной платы.

8. Условия обработки персональных данных

Обработка ПДн в Учреждении допускается в следующих случаях:

– обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

– обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

– обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

– обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения Учреждением значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн. Исключение составляет обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи;

– осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн, либо по его просьбе (далее – ПДн, сделанные общедоступными субъектом ПДн);

– осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

В случае необходимости Учреждение может включить ПДн субъектов в общедоступные источники ПДн, при этом Учреждение собирает письменное согласие субъекта на обработку его ПДн в общедоступных источниках.

Учреждение осуществляет обработку специальных категорий ПДн, касающихся состояния здоровья.

Биометрические ПДн (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Учреждением для установления личности субъекта персональных данных) в Учреждении не обрабатываются.

Учреждение не осуществляет трансграничную передачу персональных данных на территорию иностранных государств.

Принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, не осуществляется.

При отсутствии необходимости письменного согласия субъекта на обработку его ПДн согласие субъекта может быть дано субъектом ПДн или его представителем в любой позволяющей получить факт его получения форме.

Учреждение вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее – поручение). При этом Учреждение в договоре обязывает лицо, осуществляющее обработку ПДн по поручению Учреждения, соблюдать принципы и правила обработки ПДн, предусмотренные настоящей политикой и Федеральным законом РФ «О персональных данных».

В поручении определён перечень действий с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федеральным законом РФ «О персональных данных».

В случае если Учреждение поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку ПДн по поручению Учреждения, несет ответственность перед Учреждением.

Учреждение обязуется и обязывает иные лица, получившие доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

9. Права субъекта персональных данных

Субъект ПДн имеет право:

– принимать решение о предоставлении его ПДн Учреждению;

– отзывать согласие на обработку своих ПДн;

– вносить, дополнять или изменять обрабатываемые о нем ПДн;

– требовать исключить собственные ПДн из общедоступных источников ПДн;

– на получение информации, касающейся обработки его ПДн, в том числе содержащей:

– подтверждение факта обработки ПДн и правовые основания; цели и применяемые Учреждением способы обработки ПДн;

– наименование и место нахождения Учреждения, сведения о лицах (за исключением работников), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании Федеральныго закона РФ «О персональных данных»;

– обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом РФ «О персональных данных»;

– сроки обработки ПДн, в том числе сроки их хранения; порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом РФ «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом РФ «О персональных данных» или другими федеральными законами.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами РФ.

10. Обязанности Учреждения

В соответствии с требованиями Федерального закона ФЗ-152 «О персональных данных» Учреждение обязуется:

– предоставлять субъекту ПДн по его запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ;

– по требованию субъекта ПДн уточнять обрабатываемые ПДн, блокировать или удалять, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки. Либо обеспечить блокирование, удаление, в случае если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения;

– вести журнал учета обращений субъектов ПДн, в котором должны фиксироваться запросы субъектов ПДн на получение ПДн, а также факты предоставления ПДн по этим запросам;

– уведомлять субъекта ПДн об обработке ПДн в том случае, если персональные данные были получены не от субъекта ПДн (за исключением случаев, когда субъект ПДн уже уведомлен об осуществлении обработки его ПДн);

– в случае достижения цели обработки ПДн, незамедлительно прекратить обработку ПДн и уничтожить либо обезличить соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не

предусмотрено федеральными законами. Либо обеспечить уничтожение, обезличивание, в случае если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения. Уведомить об этом субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган;

– в случае отзыва субъектом ПДн согласия на обработку своих ПДн прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Учреждением и субъектом ПДн. Либо обеспечить прекращение обработки ПДн и их уничтожение, в случае если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения. Уведомить субъекта ПДн об уничтожении его ПДн;

– в случае поступления требования субъекта о прекращении обработки ПДн в целях продвижения товаров, работ, услуг на рынке немедленно прекратить обработку ПДн. Либо обеспечить прекращение обработки ПДн, в случае если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения.

11. Меры по обеспечению безопасности персональных данных

При обработке персональных данных Учреждение принимает необходимые правовые, организационные и технические меры 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.

Обеспечение безопасности ПДн достигается, в частности:

– определением угроз безопасности ПДн при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;

– учетом машинных носителей ПДн;

– обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

– восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн;

– контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

12. ИЗМЕНЕНИЕ ПОЛИТИКИ

Учреждение 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 ее размещения на сайте Учреждения, если иное не предусмотрено новой редакцией Политики.