Государственное бюджетное учреждение здравоохранения Республики Карелия «Родильный дом им. Гуткина К.А.»

УТВЕРЖДЕНО

Приказом главного врача ГБУЗ РК

«Родильный дом им. Гуткина К.А.»

от 31.12.2014г. № 432

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ РЕСПУБЛИКИ КАРЕЛИЯ

«РОДИЛЬНЫЙ ДОМ ИМ. ГУТКИНА К.А.»

Петрозаводск 2014

1.Общие положения.

1.1.Настоящее Положение об информационной безопасности персональных данных в Государственное бюджетное учреждение здравоохранения Республики Карелия «Родильный дом им. Гуткина К.А.»

(далее - Положение) определяет общие требования:

* к обработке персональных данных работников ГБУЗ РК «Родильный дом им.Гуткина К.А» и лиц, застрахованных в системе обязательного медицинского страхования (далее - персональные данные);
* к мерам по обеспечению защиты персональных данных.

1.2.Настоящее Положение разработано на основании Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.11.2010 г. №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», нормативно правовых актов и методических документов Правительства Российской Федерации, Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю, устанавливающих требования к обработке и защите персональных данных.

1.3.Настоящее Положение разработано 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;
* обеспечения соответствия законодательству Российской Федерации действий, направленных на обработку персональных данных;
* обеспечения основных направлений защиты персональных данных от несанкционированного доступа, утраты, неправомерного их использования или распространения.

1.4.Задачами настоящего Положения являются:

* определение общих принципов,порядка обработки персональных данных;
* определение основных условий обработки персональных данных, способовзащиты персональных данных;
* определение прав и обязанностей операторов и субъектов персональных данных при обработке персональных данных.

1.5.Настоящее Положение должно осуществляться в соответствии со следующими основными принципами:

* законности – соблюдение законодательства по защите персональных данных;
* эффективности и целесообразности – реализуемые мероприятия по обеспечению информационной безопасности должны сводить риски к минимуму, при этом должно учитываться соразмерность затрат на обеспечение защиты и потенциальных потерь при реализации угроз;
* непрерывности функционирования системы информационной безопасности;
* совершенствования мер и средств защиты информации;
* персональной ответственности и обязательности контроля.

1.6.Требования настоящего Положение распространяются на все структурные подразделения (отделы) ГБУЗ РК «Родильный дом им.Гуткина К.А», в которых осуществляется обработка персональных данных***.***

1.7. Государственное бюджетное учреждение здравоохранения Республики Карелия «Родильный дом им. Гуткина К.А.» (далее – ГБУЗ РК «Родильный дом им.Гуткина К.А») заключает Соглашения об информационном взаимодействии с участниками системы обязательного медицинского страхования (страховыми медицинскими организациями и медицинскими организациями), при условии соблюдения ими требований информационной безопасности, а так же иные Соглашения об обмене информацией на основании Федерального законодательства, в том числе с Министерством здравоохранения и социального развития Республики Карелия, Управлением Федеральной службы судебных приставов по Республике Карелия, Государственным учреждением - Региональным отделением Фонда социального страхования Российской Федерации по Республике Карелия, Управлением записи актов гражданского состояния Республики Карелия, Государственным учреждением - Отделением Пенсионного фонда Российской Федерации по Республике Карелия и другими.

2. Основные понятия.

2.1.В настоящем Положении используются следующие понятия и термины:

* персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
* 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. Применительно к настоящему Положению оператором является ГБУЗ РК «Родильный дом им.Гуткина К.А» (далее - Оператор);
* 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;
* автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
* распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
* предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному 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;
* информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

3.Категории субъектов персональных данных.

3.1.Оператор осуществляет обработку персональных данных следующих категорий субъектов:

* работников Оператора;
* лиц, застрахованных в системе ОМС.

4. Основные требования к обработке персональных данных.

4.1.Обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов, иных нормативных правовых актов Российской Федерации.

4.2.Общий срок обработки персональных данных определяется периодом времени, в течение которого Оператор осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки, в том числе хранения персональных данных.

4.3.Обработка персональных данных начинается с момента их получения Оператором и заканчивается:

* по достижении заранее заявленных целей обработки;
* в связи с утратой необходимости в достижении заранее заявленных целей обработки.

4.4.Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

4.5.Передача персональных данных субъекта третьей стороне не допускается без его письменного согласия, за исключением случаев, установленных законодательством.

4.6.Уточнение персональных данных, в том числе их обновление и изменение, имеет своей целью обеспечение достоверности, полноты и актуальности персональных данных.

4.6.1Уточнение персональных данных осуществляется Оператором по собственной инициативе, по требованию субъекта персональных данных, в случае, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными.

4.6.2.Об уточнении персональных данных Оператор обязан уведомить субъекта персональных данных, за исключением случаев, когда обработка персональных данных производится на основании федерального закона.

4.7. Блокирование персональных данных осуществляется Оператором по собственной инициативе, по требованию субъекта персональных данных, в случае выявления недостоверных персональных данных или неправомерных действий с ними. О блокировании персональных данных Оператор обязан уведомить субъекта персональных данных, за исключением случаев, когда обработка персональных данных производится на основании федерального закона.

4.8.Уничтожение персональных данных осуществляется:

* по достижении цели обработки персональных данных;
* в случае утраты необходимости в достижении целей обработки персональных данных;
* по требованию субъекта персональных данных.

4.9.Доступ (порядок доступа) к персональным данным, определяется отдельными локальными актами Оператора.

4.10.Оператор использует следующие способы обработки персональных данных:

* автоматизированная обработка;
* без использования средств автоматизации.

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

4.12.Особенности обработки персональных данных в зависимости от способа обработки и категории персональных данных определяются отдельными локальными актами Оператора.

4.13.Должностные лица Оператора, осуществляющие обработку персональных данных, должны быть под подпись ознакомлены с локальными актами Оператора по защите персональных данных.

5.Условия обработки персональных данных.

5.1.Обработка персональных данных осуществляется исключительно в целях выполнения функций, полномочий и обязанностей, возложенных на Оператора законодательством Российской Федерации. Обработка персональных данных в иных целях не допускается.

5.2.Общим условием обработки персональных данных Оператором является наличие письменного согласия субъектов персональных данных на осуществление такой обработки, за исключением обработки персональных данных, осуществляемой на основании федерального закона.

5.3.Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

* фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
* наименование и адрес 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 субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
* подпись субъекта персональных данных.

5.4.Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.5.Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, установленные законодательством.

5.6.Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед Оператором.

6.Конфиденциальность персональных данных.

6.1.Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.2.Обеспечение конфиденциальности персональных данных не требуется:

* в случае обезличивания персональных данных;
* в отношении общедоступных персональных данных.

6.3.Оператор и иные лица, получившие доступ к персональным данным, несут ответственность за разглашение сведений конфиденциального характера.

7.Защита персональных данных.

7.1.Оператор принимает все необходимые правовые, организационные и технические меры информационной безопасности для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

7.2.Обеспечение безопасности персональных данных обрабатываемых Оператором достигается за счет:

* определения угроз безопасности персональных данных, при их обработке в ИСПДн;
* разработки на основе модели угроз систему защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием [методов и способов](consultantplus://offline/main?base=LAW;n=97942;fld=134;dst=100009) защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
* использования шифровальных (криптографических) средств;
* учета машинных носителей персональных данных;
* установки и вводу в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
* ознакомления лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, локальными документами и актами, по вопросам обработки персональных данных
* обучения лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
* обнаружения фактов несанкционированного доступа к персональным данным и принятием мер;
* возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* установления разграничения и правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных, учет лиц, допущенных к работе с персональными данными;
* оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
* недопущения воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
* постоянного контроля за обеспечением уровня защищенности персональных данных.

8.Права субъектов персональных данных.

8.1.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 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;
* информацию об осуществленной или о предполагаемой трансграничной передаче данных;
* иные сведения, предусмотренные федеральными законами.

8.2.Субъект персональных данных 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.

8.3.Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

8.4 Решения, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

9.Обязанности Оператора при обработке персональных данных.

9.1.Оператор обязан:

9.1.1.осуществлять обработку персональных данных с соблюдением требований законодательства;

9.1.2.принимать меры, необходимые и достаточные для обеспечения безопасности персональных данных;

9.1.3.осуществлять контроль соответствия обработки персональных данных требованиям законодательства;

9.1.4.представить документы и локальные акты по запросу уполномоченного органа по защите прав субъектов персональных данных.

10. Ответственность за нарушение норм, регулирующих обработку

и защиту персональных данных

10.1.Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную ответственность, 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.