ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КРЫМ « КРЫМСКИЙ РЕСПУБЛИКАНСКИЙ ЦЕНТР МЕДИЦИНЫ КАТАСТРОФ И СКОРОЙ МЕДИЦИНСКОЙ ПОМОЩИ»

УТВЕРЖДЕНО
ПРИКАЗОМ ГБУЗ РК «КРЦМК и СМП»

от « 06 » февраля 2015г. № 68

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

1. Общие положения

1.1. Государственное бюджетное учреждение здравоохранения Республики Крым «Крымский республиканский центр медицины катастроф и скорой медицинской помомщи» — далее «Центр», являясь Работодателем (оператором), осуществляет работу с персональными данными сотрудников Центра, в соответствии с нормами Конституции Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также общепризнанными принципами и нормами международного права и международных договоров РФ, которые в соответствии с частью четвертой ст.15 Конституции РФ являются составной частью российской правовой системы.

1.2. Цель Положения:

1.2.1. Защита персональных данных от несанкционированного доступа третьих лиц и организация приема, хранения, обработки и передачи персональных данных сотрудников осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Режим конфиденциальности:

1.3.1.Сбор, хранение, использование и распространение информации о частной жизни Работника без его письменного согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.

1.3.2. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 летнего срока хранения, если иное не определено законодательством РФ.

1.4. Порядок утверждения данных правил, ввода их в действие и внесения изменений утверждаются директором Центра и вводятся в действие его приказом.

2. Понятие и состав персональных данных

2.1. Понятие персональных данных

Персональные данные Сотрудника - это любая информация, необходимая Работодателю в связи с трудовыми отношениями или полученная им на основании письменного согласия Сотрудника, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное

положение, образование, профессия, доходы, другая информация. Если по совокупности сведений определить их принадлежность к конкретному субъекту невозможно, то данные сведения не относятся к персональным данным.

Обработка персональных данных Сотрудника - это любое действие, совершаемое 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 и должна осуществляться на законной и справедливой основе.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений, порождающих юридические последствия в отношении субъекта персональных данных затрагивающих права и свободы субъекта персональных данных или других лиц.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

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.

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

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;

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия персональных данных.

3. Сбор, обработка и хранение персональных данных

3.1. Порядок получения персональных данных:

а) обработка персональных данных сотрудников осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия Работникам, в выполнении им своих служебных обязанностей.

б) персональные данные следует получать лично у сотрудников. В случае возникновения необходимости получения персональных данных Работников у третьей стороны следует известить об этом сотрудника заранее, получить его письменное согласие и сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных;

в) запрещается получать, обрабатывать и приобщать к личному делу сотрудника не

установленные законом РФ от 27 июля 2006 г. N 152-ФЗ "О персональных данных" персональные данные о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

г) при принятии решений, затрагивающих интересы Работника, запрещается основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

д) защита персональных данных сотрудника от неправомерного их использования или утраты обеспечивается за счет средств в порядке, установленном Федеральным законом, от 27 июля 2006 г. N 152-ФЗ "О персональных данных", Трудовым кодексом;

е) передача персональных данных Работника третьей стороне не допускается без письменного согласия Работника, за исключением случаев, установленных федеральными законами;

ж) обеспечение конфиденциальности персональных данных, за исключением случаев их обезличивания;

з) в случае выявления недостоверных персональных данных Работника или неправомерных действий с ними оператора при обращении или по запросу Работника, являющегося субъектом персональных данных, или его законного представителя, оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему Работнику, с момента такого обращения или получения такого запроса на период проверки;

и) в случае подтверждения факта недостоверности персональных данных сотрудника оператор на основании документов, представленных работником, обязан уточнить персональные данные и снять их блокирование;

к) в случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить Работника, являющегося субъектом персональных данных, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;

л) хранение персональных данных должно осуществляться в форме, позволяющей определить работника, являющегося субъектом персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

м) обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме Работника, являющегося субъектом персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

н) трансграничная передача персональных данных на территории иностранных государств осуществляется в соответствии с Федеральным законом от 27 июля 2006г. N 152-ФЗ "О персональных данных".

3.2. Состав сотрудников, допущенных к обработке, передаче и хранению персональной информации.

3.2.1. **Полный доступ:** к обработке персональных данных сотрудника исходя из функциональных обязанностей должностных лиц имеют следующие сотрудники:

- директор;
- заместители директора;
- главные врачи станций скорой медицинской помощи;
- главный бухгалтер;
- отдел правового обеспечения;
- отдел кадров;
- системный администратор;
- ответственный за техническую защиту информации по Центру

3.2.2. Ограниченный доступ к обработке персональных данных Работника исходя из функциональных и должностных обязанностей имеют следующие сотрудники:

Наименование должности	**Персональные данные и перечень документов, к которым может быть допущен. А также цели, для которых данное должностное лицо имеет право обрабатывать данные сведения**
Секретарь директора и работники канцелярии	- адрес места жительства и контактные телефоны работников для оперативного оповещения и передачи служебной информации Работнику;
Бухгалтер по расчету заработной платы	- сведения об иждивенцах — для произведения необходимых вычетов из заработной платы, установленных законодательно; - ИНН, номер страхового свидетельства государственного пенсионного страхования, адрес места прописки — для оформления бухгалтерской, налоговой, статистической отчетности;

3.3. Порядок обработки, передачи и хранения персональной информации.

3.3.1. В соответствии со ст.86 ТК РФ в целях обеспечения прав и свобод гражданина Работодатель и его представители при обработке персональных данных Сотрудника должны соблюдать следующие общие требования:

• обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

В целях обеспечения защиты персональных данных, хранящихся у Работодателя, работники имеют право на:

• полную информацию об их персональных данных и обработке этих данных;

• свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Работника, за исключением случаев, предусмотренных федеральным законом;

• определение своих представителей для защиты своих персональных данных;

• доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

• требование об извещении Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

• обжалование в суде любых неправомерных действий или бездействия

Работодателя при обработке и защите его персональных данных.

3.4. Ответственность за разглашение персональных данных

3.4.1. Все лица, непосредственно имеющие отношение к персональной базе данных, должны подписывать обязательство о неразглашении персональной информации работников.

3.4.2. **Персональная ответственность** — одно из главных требований в организации функционирования системы защиты персональной информации.

3.4.3. Директор, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

3.4.4. Каждый сотрудник Центра, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

3.4.5. Ответственность лиц, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, согласно действующему законодательству может быть привлечен к дисциплинарной, административной, гражданско-правовой или уголовной ответственности в соответствии с федеральными законами.

3.4.6. Должностные лица, допущенные к обработке персональных данных работников, в случае их разглашения могут быть уволены по инициативе Работодателя по ст. 81 часть первая пункт 6 «в» Трудового кодекса РФ. То есть разглашение персональных данных Работника, ставших известным должностным лицам в связи с исполнением должностных обязанностей, является грубым нарушением должностных обязанностей.

4. Доступ к персональным данным

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным сотрудника имеют лица, указанные в п. 3.2 данного положения. Другие сотрудники Центра имеют доступ к персональным данным сотрудника только с письменного согласия самого сотрудника.

4.1.2. По письменному заявлению сотрудника Работодатель обязан не позднее трех рабочих дней со дня подачи этого заявления выдать работнику копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы; выписки из трудовой книжки; справки о своей заработной плате и т.д.

Копии документов, связанных с работой, должны быть заверены надлежащим образом и представляться работнику безвозмездно.

4.2. Внешний доступ.

4.2.1. К числу лиц, допущенных к персональным данным сотрудника, имеют организации, осуществляющие контрольные и надзорные функции, а именно:

- инспекции по труду;
- прокуратура РФ;
- правоохранительные органы;
- налоговые инспекции;
- военкоматы;
- органы, осуществляющие миграционный учет иностранных граждан;
- органы ФСС РФ;
- органы Пенсионного фонда РФ;

4.2.3. Органы и должностные лица, указанные в п. 4.2.1, имеют доступ к информации только в сфере своей компетенции в порядке, установленном законодательством РФ.

4.2.4. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к

персональным данным Работника только в случае письменного разрешения Работника.

4.2.5. Сведения о работающем Работнике или уже уволенном могут быть предоставлены другой организации только на основании письменного запроса, оформленного на бланке организации, с приложением копии нотариально заверенного заявления Работника, содержащего согласие на передачу указанным лицам его сведений, с полным указанием того, какие сведения могут быть переданы на основании данного согласия.

4.2.6. Родственники и члены семьи сотрудника:

- персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Работника. В случае развода и отсутствия соглашения сторон об уплате алиментов справка о заработной плате Работника может быть предоставлена в суд без его согласия на основании письменного запроса и определения суда.

5. Защита персональных данных

Терминология используемая в положении:

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных.

5.1. Внутренняя защита

5.1.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных.

Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

Для защиты персональных данных сотрудников работодатель принимает следующие меры:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое распределение документов и информации между сотрудниками. Порядок работы с документами, содержащими персональные данные Работника, регламентирован законодательством Российской Федерации и настоящим Положением;
- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание Работником требований нормативно-методических документов по защите информации и сохранении тайны. Для этого со всеми работниками, допущенными к персональным данным, проводятся при допуске и периодически соответствующие инструктаж и обучение;
- наличие необходимых условий, исключающих несанкционированный доступ в помещения для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника.