МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КРЫМ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КРЫМ
« СИФЕРОПОЛЬСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА»
ГБУЗ РК «СИМФЕРОПОЛЬСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА»
295043 г. Симферополь, ул. Киевская 142,тел. 66-30-00

« 19 » 08 2019 года № 279

«Об утверждении и введении в действие положения о работе с персональными данными работников и пациентов ГБУЗ РК «Симферопольская клиническая больница»»

ПРИКАЗ

Во исполнение требований главы 14 Трудового кодекса «Защита персональных данных работника» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение о работе с персональными данными работников и пациентов ГБУЗ РК «Симферопольская клиническая больница» (Прилагается).
2. Начальнику отдела кадров Омельченко В.Ю. в срок до 16 сентября 2019 года ознакомить всех работников ГБУЗ РК «Симферопольская клиническая больница» под подпись с Положением о работе с персональными данными.
3. Возложить персональную ответственность за разглашение персональных данных работников и пациентов ГБУЗ РК «Симферопольская клиническая больница» на работников, замещающих должность:
   - заместителей главного врача;
   - начальника отдела кадров;
   - специалистов отдела кадров;
   - начальника контрактной службы;
   - главного бухгалтера;
   - заместителя главного бухгалтера;
   - секретаря руководителя;
   - бухгалтеров отдела бухгалтерского учета и отчетности (расчетный отдел и касса);

- юрисконсульта;
- экономиста планово-экономического отдела;
- главная медицинская сестра
- медицинских регистраторов;
- заведующую поликлиникой;
- старших медицинских сестер и иных сотрудников при установлении данного факта

4.Секретарю руководителя ознакомить с данным приказом всех причастных лиц.

5. Общий контроль за организацией работы с персональными данными работников и пациентов ГБУЗ РК «Симферопольская клиническая больница» возложить на заместителя главного врача по безопасности Долгих А.А.

Главный врач **Курдес О.А.**

Согласовано:

«УТВЕРЖДАЮ»
Главный врач
ГБУЗ РК «Симферопольская клиническая больница»
_____ О.А. Курдес
«19» августа 2019 г.

ПОЛОЖЕНИЕ
о порядке хранения и защиты персональных данных работников и пациентов ГБУЗ РК «Симферопольская клиническая больница»

1.1. Настоящее Положение определяет порядок обработки (получения, использования, хранения, уточнения (обновления, изменения), распространения (в том числе передачи), обезличивания, блокирования, уничтожения, защиты) персональных данных работников и пациентов Государственного бюджетного учреждения здравоохранения Республики Крым «Симферопольская клиническая больница» (далее — Учреждение), а также гарантии обеспечения конфиденциальности сведений о них.

1.2. Настоящее Положение разработано на основании: Конституции Российской Федерации, Гражданского кодекса Российской Федерации, Трудового кодекса Российской Федерации, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Указа Президента РФ от 06 марта 1997 г. № 188 (ред. от 23 сентября 2005 г.) «Об утверждении перечня сведений конфиденциального характера»; Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других действующих нормативных правовых актов Российской Федерации.

1.3. Цель настоящего Положения - защита персональных данных работников и пациентов Учреждения от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

1.4. Требования настоящего Положения распространяются на всех работников и пациентов Учреждения.

1.5. Настоящее Положение и изменения к нему утверждаются Главным врачом Учреждения и вводятся приказом и являются обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным сотрудников и пациентов. Все работники предприятия должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

2. ОСНОВНЫЕ ПОНЯТИЯ

В настоящем Положении используются следующие понятия и термины:

работник — физическое лицо, вступившее в трудовые отношения с работодателем ГБУЗ РК «Симферопольская клиническая больница»;

работодатель – ГБУЗ РК «Симферопольская клиническая больница»;

пациенты - лица, обратившиеся за медицинской помощью, находящиеся под медицинским наблюдением, лица – получатели платных медицинских услуг, состоящие в договорных отношениях с ГБУЗ РК «Симферопольская клиническая больница»;

субъекты персональных данных — работники и пациенты ГБУЗ РК «Симферопольская клиническая больница»;

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;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки 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;

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 или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

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 субъекта персональных данных или наличия иного законного основания;

трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

информация — сведения (сообщения, данные) независимо от формы их представления;

доступ к информации — возможность получения информации и ее использования.

3. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу.

3.2. Состав персональных данных работников и пациентов, обработку которых осуществляет Учреждение:

- фамилия, имя, отчество;
- год рождения; месяц рождения; дата рождения, место рождения;
- пол;
- гражданство;
- анкетные и биографические данные;
- образование;
- профессия, доходы;

- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- сведения об аттестации;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- размер заработной платы;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным работника;
- рекомендации, характеристики;
- деловые и иные личные качества, которые носят оценочный характер;
- СНИЛС;
- ИНН;
- состояние здоровья;
- место работы; полис ОМС;
- полис ДМС либо номер договора;
- дата и время поступления в Учреждение;
- дата и время выписки из Учреждения;
- прочие сведения, которые могут идентифицировать человека.

Из указанного списка Учреждение вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора (эффективного контракта), а также которые характеризуют гражданина как пациента Учреждения.

3.3. Данные документы являются конфиденциальными. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

3.4. Учреждение осуществляет обработку персональных данных следующих категорий субъектов:

- работников, состоящих в трудовых отношениях с Учреждением;
- пациентов Учреждения и их ближайших родственников;
- физических лиц – посетителей сайта Учреждения – https://simf-klin-bolnica.ru

3.5. Информация о персональных данных может содержаться:

- на бумажных носителях;
- на электронных носителях;
- в информационно-телекоммуникационных сетях и иных информационных системах Учреждения.

3.6. Учреждение использует следующие способы обработки персональных данных:

автоматизированная обработка;

без использования средств автоматизации;

смешанная обработка (с применением объектов вычислительной техники).

Учреждение самостоятельно устанавливает способы обработки персональных данных в зависимости от целей такой обработки и материально-технических возможностей Учреждения.

При обработке персональных данных с применением объектов вычислительной техники должностные лица, осуществляющие такую обработку (пользователи объектов вычислительной техники), должны быть ознакомлены под роспись с локальными нормативными актами Учреждения, устанавливающими порядок применения объектов вычислительной техники в Учреждении.

3.7. Персональные данные работников Учреждения содержатся в следующих документах (копиях указанных документов):

- заявления работников (о принятии на работу, об увольнении и т.п.);
- паспорт (или иной документ, удостоверяющий личность);
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учёт в налоговый орган и присвоении ИНН;
- документы воинского учёта;
- документы об образовании, о квалификации или наличии специальных знаний, специальной подготовки;
- карточка Т-2;
- личный листок по учету кадров
- медицинское заключение о состоянии здоровья, индивидуальная программа реабилитации, медицинская справка о прохождении медицинских осмотров;
- документы, содержащие сведения об оплате труда (расчетный листок);

- другие документы, содержащие персональные данные и предназначенные для использования в служебных целях.

3.8. Персональные данные пациентов Учреждения содержатся в следующих документах:

- Медицинская карта стационарного и амбулаторного больного (медицинская справка, результаты анализов, врачебно-консультативное заключение, протоколы заседания ВКК, пр.);
- Договор на оказание платных медицинских услуг;
- другие документы, содержащие персональные данные пациентов.

4. ОБЯЗАННОСТИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекты персональных данных обязаны:

4.1. Передавать Учреждению или его представителю комплекс достоверных документированных персональных данных.

4.2. Своевременно в разумный срок, не превышающий 5 дней, сообщать Учреждению об изменении своих персональных данных (смена фамилии, паспортных данных, сведения об образовании и т.п.).

5. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъекты персональных данных имеют право:

5.1. На полную информацию о своих персональных данных и обработке этих данных.

5.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.3. На доступ к медицинским данным с помощью медицинского специалиста по своему выбору.

5.4. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований, определенных трудовым законодательством. При отказе Учреждения исключить или исправить персональные данные субъекта персональных данных он имеет право заявить в письменной форме Учреждению о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.5. Требовать извещения Учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.6. Обжаловать в суд любые неправомерные действия или бездействие Учреждения при обработке и защите его персональных данных.

5.7. Определять своих представителей для защиты своих персональных данных.

6. СБОР, ОБРАБОТКА И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. 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 работника либо пациента Учреждения.

6.2. Все персональные данные субъекта персональных данных следует получать у него самого. Если персональные данные работника либо пациента Учреждения возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

6.3. Учреждение должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

6.4. Работник либо пациент Учреждения представляет Учреждению достоверные сведения о себе. Учреждение проверяет достоверность сведений, сверяя данные, представленные работником, либо пациента Учреждения, с имеющимися у него документами. Представление работником Учреждения подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

6.5. Документы, содержащие персональные данные, создаются/получают путём:

- копирования оригиналов (паспорт, свидетельство ИНН, свидетельство государственного пенсионного страхования, страховой медицинский полюс др.);
- внесения сведений в учётные формы (на бумажных и электронных носителях);
- получения оригиналов необходимых документов (трудовая книжка, личный листок по учёту кадров, автобиография, др.).
- внесения в информационные системы Учреждения.

6.6. Правовыми основаниями обработки персональных данных работников Учреждения выступают трудовое законодательство РФ и иные нормативные правовые акты, содержащие нормы трудового права, пациентов — законодательство РФ, лицензия на осуществление медицинской деятельности, гражданско-правовые договоры, также согласие субъекта персональных данных.

6.7. Общий срок обработки персональных данных определяется периодом времени, в течение которого Учреждение осуществляет действия (операции) в

отношении персональных данных, обусловленные заявленными целями их обработки, в том числе хранение персональных данных.

Сроки хранения документов, содержащих персональные данные, в Учреждении установлены действующим законодательством. Документы, содержащие персональные данные, с неустановленными сроками хранения уничтожаются по достижению цели обработки.

6.8. Обработка персональных данных начинается с момента их получения Учреждением и заканчивается: по достижении заранее заявленных целей обработки; либо по факту утраты необходимости в достижении заранее заявленных целей обработки.

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

6.10. Обработка персональных данных субъекта персональных данных без получения его согласия осуществляется в следующих случаях, предусмотренных законодательством Российской Федерации.

6.11. Обработка персональных данных осуществляется только должностными лицами Учреждения, непосредственно использующими их в служебных целях.

Уполномоченные администрацией Учреждением на обработку персональных данных лица (операторы) имеют право получать только те персональные данные, которые необходимы для выполнения своих должностных обязанностей. Все остальные работники и пациенты Учреждения имеют право на полную информацию, касающуюся только собственных персональных данных.

6.12. Хранение информации о начислении заработной платы работников ГБУЗ РК «Симферопольская клиническая больница» осуществляется на электронных и бумажных носителях. Распространение данной информации третьим лицам, без письменного согласия конкретного работника, запрещается.

7. УТОЧНЕНИЕ, БЛОКИРОВАНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

7.2. Уточнение персональных данных осуществляется Учреждением по собственной инициативе, по требованию субъекта персональных данных или его законного представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными.

Об уточнении персональных данных Учреждением обязано уведомить субъекта персональных данных или его законного представителя.

7.3. Блокирование персональных данных осуществляется Учреждением по требованию субъекта персональных данных или его законного представителя, а также по требованию уполномоченного органа по защите прав субъектов

персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними.

О блокировании персональных данных Учреждением обязано уведомить субъект персональных данных или его законного представителя.

7.4. 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 или уполномоченного органа по защите прав субъектов персональных данных в случае выявления фактов совершения Учреждением неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.

7.5. В целях обеспечения законности при обработке персональных данных и устранения факторов, влекущих или могущих повлечь неправомерные действия с персональными данными, Учреждение вправе по собственной инициативе осуществить блокирование и (или) уничтожение персональных данных.

О блокировании и (или) уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его законного представителя.

8. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. При передаче персональных данных субъекта персональных данных Учреждение должно соблюдать следующие требования:

- не сообщать персональные данные субъекта персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъекта персональных данных, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта персональных данных, обязаны соблюдать конфиденциальность. Данное положение не распространяется на обмен персональными данными субъекта персональных данных в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным субъекта персональных данных только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъекта персональных данных, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать персональные данные субъекта персональных данных представителям субъекта персональных данных в порядке, установленном действующим законодательством Российской Федерации, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций;

- передавать персональные данные о начислении заработной платы работника ГБУЗ РК «Симферопольская клиническая больница», лично работнику, указанному в расчетном листке (либо по доверенности – третьему лицу), с отметкой о получении (подпись в специальном журнале).

Ответственным за начисления заработной платы работникам ГБУЗ РК «Симферопольская клиническая больница» запрещается передавать данные о размере заработной платы других работников ГБУЗ РК «Симферопольская клиническая больница», без их письменного согласия, третьим лицам.

9. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

9.1. Внутренний доступ (доступ внутри организации).

9.1.1. Право доступа к персональным данным работника имеют:

- главный врач;
- заместители главного врача;
- главный бухгалтер;
- заместитель главного бухгалтера;
- начальник отдела кадров, специалисты по кадрам;
- экономисты;
- инженер-программист;
- операторы ЭВМ;
- главная медицинская сестра;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников подразделения);
- при переводе из одного структурного подразделения в другое доступ к персональным данным сотрудника может иметь руководитель нового подразделения по согласованию с руководителем предприятия;
- сотрудники бухгалтерии;
- специалист по охране труда – к тем данным, которые необходимы для выполнения конкретных функций;
- секретарь руководителя – к тем данным, которые необходимы для выполнения конкретных функций;
- сам работник, носитель данных.

Другие сотрудники организации имеют доступ к персональным данным работника только с письменного согласия самого работника, носителя данных.

9.1.2. Доступ к персональным данным пациентов имеют следующие должностные лица Учреждения, непосредственно использующие их в рамках выполнения своих должностных обязанностей:

- Главный врач;

- Заместители главного врача;
- Главный бухгалтер;
- Инженер-программист, оператор ЭВМ, экономист непосредственно обрабатывающие персональные данные пациентов;
- Сотрудники бухгалтерии;
- Секретарь руководителя - к тем данным, которые необходимы для выполнения конкретных функций;
- юрисконсульт – к тем данным, которые необходимы для выполнения конкретных функций
- Врачебный персонал (заведующие отделениями, врачи);
-Средний медицинский персонал, в т.ч. медицинские регистраторы

9.2. Внешний доступ.

Персональные данные вне организации могут представляться в государственные и негосударственные функциональные структуры:
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения государственных и муниципальных органов управления.

9.3. Другие организации.

Сведения о работнике (в том числе уволенном) и пациенте могут быть предоставлены другой организации (учреждению, ведомству) только с письменного запроса на бланке организации с приложением копии согласия субъекта персональных данных.

9.4. Родственники и члены семей.

Персональные данные работника и пациента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта персональных данных.

9.5. Перечень работников Учреждения, имеющих в силу исполнения ими своих должностных обязанностей доступ к персональным данным, утверждается приказом главного врача Учреждения.

10. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. В целях обеспечения сохранности и конфиденциальности персональных данных субъектов персональных данных Учреждения все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

10.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке предприятия и в том объеме, который позволяет не разглашать излишний объем персональных сведений о работниках предприятия.

10.3. Передача информации, содержащей сведения о персональных данных субъектов персональных данных Учреждения, по телефону, факсу, электронной почте (по не защищенным каналам связи) без письменного согласия субъектов персональных данных запрещается.

10.4. Личные дела и документы, содержащие персональные данные субъектов персональных данных, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

10.5. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

10.6. Персональные данные в зависимости от способа их фиксации (бумажный носитель, электронный носитель) подлежат обработке таким образом, чтобы исключить возможность ознакомления с содержанием указанной информации сторонними лицами.

11. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

11.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законам.

Приложение № 1 к приказу
от 01 июля 2019 №

«УТВЕРЖДАЮ»
Главный врач ГБУЗ РК
«Симферопольская клиническая больница»
_____О.А. Курдес
«___» _____ 2019 г.

ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности

АННОТАЦИЯ

Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в ГБУЗ РК «Симферопольская клиническая больница».

Инцидент - одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее - ИС) и (или) к возникновению угроз безопасности, в том числе персональных данных.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Положение о работе с инцидентами информационной безопасности (далее – Положение) разработано в соответствии с:

- Федеральным законом № 152-ФЗ «О персональных данных»;
- Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановлением Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- политикой информационной безопасности ГБУЗ РК «Симферопольская клиническая больница скорой медицинской помощи №6».

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

Работа с инцидентами включает в себя следующие направления:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;

- обнаружение, идентификация и регистрация инцидентов;

- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;

- принятие мер по устранению последствий инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий; планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в соответствии с приказом главного врача.

2. ОТВЕТСТВЕННЫЕ ЗА ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И РЕАГИРОВАНИЕ НА НИХ

2.1. В информационных системах.

Ответственными за выявление инцидентов в ИС являются:

- лица, имеющие право доступа к ИС;
- ответственный за техническое обслуживание ИС;
- администратор ИС;
- администратор информационной безопасности ИС.

Ответственными за реагирование на инциденты в ИС являются:

- лица, имеющих право доступа к ИС;
- руководитель подразделения ГБУЗ РК «Симферопольская клиническая больница», в котором выявлен инцидент;
- ответственный за техническое обслуживание ИС;
- администратор ИС;
- администратор информационной безопасности ИС;
- ответственный за организацию обработки персональных данных Учреждения, в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);
- Председатель комиссии по работе с инцидентами.

2.2. Вне информационных систем.

Ответственными за выявление инцидентов вне ИС являются все сотрудники ГБУЗ РК «Симферопольская клиническая больница».

Ответственными за реагирование на инциденты вне ИС являются:

- сотрудник ГБУЗ РК «Симферопольская клиническая больница» , обнаруживший инцидент;

- руководитель подразделения ГБУЗ РК «Симферопольская клиническая больница», в котором выявлен инцидент;

- ответственный за организацию обработки персональных данных ГБУЗ РК «Симферопольская клиническая больница», в случае, если существует угроза безопасности персональных данных;

- председатель комиссии по работе с инцидентами.

3. ОБНАРУЖЕНИЕ, ИДЕНТИФИКАЦИЯ И РЕГИСТРАЦИЯ ИНЦИДЕНТОВ

3.1 Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- выявление инцидентов в области информационной безопасности с помощью технических средств;

- выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

- выявление инцидентов с помощью сотрудников ГБУЗ РК «Симферопольская клиническая больница»

3.2 Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- доведение до сотрудников ГБУЗ РК «Симферопольская клиническая больница» информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет заместитель главного врача по безопасности А.А. Долгих в журнале регистрации инцидентов информационной безопасности. Форма журнала утверждается приказом главного врача ГБУЗ РК «Симферопольская клиническая больница».

Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение ведение и хранение журнала – заместитель главного врача по безопасности А.А. Долгих.

4. ИНФОРМИРОВАНИЕ О ВОЗНИКНОВЕНИИ ИНЦИДЕНТОВ

Работник ГБУЗ РК «Симферопольская клиническая больница» (пользователь), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, Администратору ИС, Администратору информационной безопасности ИС, Ответственному за организацию обработки персональных данных (в случае если ИС является ИСПДн), Председателю комиссии по работе с инцидентами.

Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

5. АНАЛИЗ ИНЦИДЕНТОВ, А ТАК ЖЕ ОЦЕНКА ИХ ПОСЛЕДСТВИЙ

Анализ инцидентов, в том числе определение источников и причин

возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

5.1. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

- действия организаций и отдельных лиц враждебные интересам ГБУЗ РК «Симферопольская клиническая больница» ;
- отсутствие персональной ответственности сотрудников ГБУЗ РК «Симферопольская клиническая больница» и их руководителей за обеспечение информационной безопасности, в том числе персональных данных;
- недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;
- отсутствие моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;
- недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;
- совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;
- наличие привилегированных бесконтрольных пользователей в информационной системе;
- пренебрежение правилами и требованиями информационной безопасности сотрудниками ГБУЗ РК «Симферопольская клиническая больница» ;
- и другие причины.

5.2. Оценка последствий инцидента производится на основании потенциально-возможного ущерба.

6. ПРИНЯТИЕ МЕР ПО УСТРАНЕНИЮ ПОСЛЕДСТВИЙ ИНЦИДЕНТОВ

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

- определение границ инцидента и ущерба от реализации угроз информационной безопасности;
- ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. ПЛАНИРОВАНИЕ И ПРИНЯТИЕ МЕР ПО ПРЕДОТВРАЩЕНИЮ ИНЦИДЕНТОВ

7.1. Планирование и принятие мер по предотвращению повторного возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

- планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками ГБУЗ РК «Симферопольская клиническая больница»;
- проведении мероприятий по обучению сотрудников ГБУЗ РК

«Симферопольская клиническая больница» правилам и способам работы со средствами защиты информационных систем;

- доведении до сотрудников норм законодательства, внутренних документов ГБУЗ РК «Симферопольская клиническая больница», устанавливающих ответственность за нарушение требований информационной безопасности;

- разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимаемыми на работу;

- своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности;

- своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал ГБУЗ РК «Симферопольская клиническая больница» является важным источником сведений об инцидентах информационной безопасности, поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются основанием для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Заместитель главного врача
по безопасности А.А. Долгих