УТВЕРЖДАЮ

Директор ОАО «МЦ «Гиппократ»

А.Ю. Звонков

2015г.

Положение

об организации работы с персональными данными и о защите персональных данных

в открытом акционерном обществе «Медицинский центр «Гиппократ»

1. Общие положения

1.1. Настоящее Положение устанавливает для **оператора персональных данных, каковым является открытое акционерное общество «Медицинский центр «Гиппократ»,** требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

1.2. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных работников Общества, ведения их личных дел в соответствии с трудовым законодательством Российской Федерации, а также порядок получения, обработки, хранения, передачи и любого другого использования персональных данных клиентов - Заказчиков по договорам оказания возмездных медицинских услуг, физических лиц по заключенным Обществом гражданско-правовым договорам, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и от иных субъектов персональных данных.

1.3. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ от 30.12.2001 г. N 197-ФЗ (14 глава, с изменениями и дополнениями),

Федеральным законом РФ от 19.12.2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»,

Федеральным законом РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»,

Постановлением Правительства РФ от 17.11.2007 г. N781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке *в* информационных системах персональных данных»,

Постановлением Правительства РФ от 15.09.2008 г. N687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

Постановлением Правительства РФ! от 15.08.2006г. N504 «О лицензировании деятельности по технической защите конфиденциальной информации»,

Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»,

Приказом Россвязькомнадзора от 17.07-2008 г. N08 «Об утверждении образца формы уведомления об обработке персональных данных»,

Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.97 № 188,

А также в соответствии с методическими документами ФСТЭК России (документы ДСП): «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 года,

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года, «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года, «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года и другими нормативными правовыми актами Российской Федерации.

На основании указанных выше документов всеми организациями и физическими лицами на территории Российской Федерации должен обеспечиваться требуемый уровень безопасности персональных данных

1.4. Законодательством Российской Федерации ответственность за надлежащую защиту персональных данных возлагается на организации, в которых персональные данные обрабатываются. Уполномоченным органом по контролю за соблюдением законодательства о персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

1.5. В настоящем Положении используются следующие термины и определения:

Под персональными данными (ПД) понимают любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор персональных данных •) государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

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 наличия таких средств

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.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации.

Работник — физическое лицо, состоящее в трудовых отношениях с работодателем.

Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (сведения о фактах, событиях и обстоятельствах частной жизни).

Обработка персональных данных работника — получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

Защита персональных данных работника — деятельность управомоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации **о** конкретном работнике, полученной работодателем в связи с трудовыми отношениями.

Конфиденциальная информации - это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.

1.6. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей **организационные меры и средства защиты информации** (в том числе шифровальные (криптографические) средства, **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.**

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

1.7. Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий. Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

1.8. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

1.9. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

1.10. Информационные системы классифицируются Обществом как юридическим лицом, организующим и (или) осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных (далее - оператор), в зависимости от объема обрабатываемых персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных

технологий и связи Российской Федерации - Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. N55/86/20 *«Об* утверждении Порядка проведения классификации информационных систем персональных данных».

1.11. **Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.**

1.12. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

1.13. Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

2. Сбор, обработка и защита персональных данных работника

2.1. Персональные данные работника относятся к конфиденциальной информации, то есть порядок работы с ними регламентирован действующим законодательством РФ и осуществляется с соблюдением строго определенных правил и условий. Данные требования установлены ст. 86 Трудового кодекса РФ и не подлежат изменению, исключению, так как являются обязательными для сторон трудового отношения.

2.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

2.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества работодателя, работника и третьих лиц;

2.2.2. При определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами;

2.2.3. Все персональные данные работника следует получать лично у работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее **и от него должно быть получено письменное согласие.** Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса на прежнее место работы работника в целях выяснения его профессиональных качеств; запроса в учебное заведение о подлинности документа об образовании и т.п.) и последствиях отказа работника дать письменное согласие на их получение;

2.2.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

2.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

2.2.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных или в результате

электронной автоматизированной обработки.

2.3. При поступлении на работу работник предоставляет персональные данные о себе в документированной форме. А именно:

—паспорт или иной документ, удостоверяющий личность;

—трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;

—страховое свидетельство государственного пенсионного страхования;

—документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу:

—документ об образовании, о квалификации или наличии специальных знаний при поступлении на работу, требующую специальных знаний или специальной подготовки;

—в отдельных случаях с учетом специфики работы действующим законодательством РФ может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов (например, медицинское заключение для лиц в возврате до 18 лет; для лиц, занятых на тяжелых работах и работах с вредными и (или) опасными условиями труда, а также на работах, связанных с движением транспорта).

2.4. Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

2.5. При заключении трудового договора и в ходе трудовой деятельности может возникнуть необходимость в предоставлении работником документов:

—о возрасте детей;

—о беременности женщины;

—об инвалидности;

—о донорстве;

—о составе семьи;

—о доходе с предыдущего места работы;

—о необходимости ухода за больным членом семьи;

—прочие.

2.6. После того, как будет принято решение о приеме работника на работу, а также впоследствии в процессе трудовой деятельности к документам, содержащим персональные данные работника, также будут относиться:

—трудовой договор и приказ о приеме на работу;

—приказы о поощрениях и взысканиях;

—приказы об изменении условий трудового договора;

—карточка унифицированной формы Т-2, утвержденная постановлением

Госкомстата России от 05.01.04 № 1;

—другие документы.

2.7. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом не менее чем за три рабочих дня и от него должно быть получено письменное согласие (либо письменный отказ), которое работник должен дать в течение пяти рабочих дней с момента получения от работодателя соответствующего уведомления.

В письменном уведомлении работодатель должен поставить работника в известность о последствиях отказа в даче им согласия на получение персональных данных, включая отказ в приеме на работу.

2.8. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

2.9. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ, иными федеральными законами.

2.10. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки

персональных данных работников, а также осведомлены об их правах и обязанностях в этой области.

2.11. Работники не должны отказываться от своих прав на сохранение и защиту тайны. Если в трудовом договоре будет содержаться норма об отказе работника от

данного права, то в этой части трудовой договор будет считаться недействительным.

2.12. Работодатели, работники и их представители должны совместно вырабатывать меры зашиты персональных данных работников.

3. Хранение персональных данных работника

3.1. Сведения о работниках Общества хранятся на бумажных носителях в помещении отдела кадров. Для этого используются специально оборудованные шкафы и сейфы, которые запираются и опечатываются. Сведения о работниках располагаются в алфавитном порядке. Ключи от шкафов и сейфов, в которых хранятся сведения о работниках Общества, находятся у начальника отдела кадров, а при его отсутствии — у назначенного директором лица из числа работников Общества. Личные дела уволенных работников хранятся в архиве отдела кадров в алфавитном порядке.

3.2. Конкретные обязанности по хранению личных дел работников, заполнению, хранению и выдаче трудовых книжек (дубликатов трудовых книжек), иных документов, отражающих персональные данные работников, возлагаются на начальника отдела кадров и закрепляются в его должностной инструкции.

3.3. В отношении некоторых документов действующим законодательством РФ могут быть установлены иные требования хранения, чем предусмотрено настоящим Положением. В таких случаях следует руководствоваться правилами, установленными соответствующим нормативным актом.

3.4. Сведения о работниках Общества могут также храниться на электронных носителях, доступ к которым ограничен личным паролем начальника отдела кадров.

3.5. Работодатель обеспечивает ограничение доступа к персональным данным работников лицам, не уполномоченным законом либо работодателем для получения соответствующих сведений.

3.6. Доступ к персональным данным работников без специального разрешения имеют работники, занимающие в организации следующие должности:

—директор;

—заместитель директора по организации здравоохранения;

—главный бухгалтер;

—начальник отдела кадров;

—юрист.

3.7. При получении сведений, составляющих персональные данные работника, указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций, заданий.

4. Передача персональных данных работника

4.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом (например, несчастный случай на производстве обязывает работодателя при необходимости доставить пострадавшего в учреждение здравоохранения, немедленно проинформировать родственников пострадавшего, а также направить сообщение в органы и организации, определенные Трудовым кодексом РФ (ст. 228 ТК РФ), иными федеральными законами; о случаях острого отравления работодатель сообщает в соответствующий орган санитарно-эпидемиологического надзора).

Учитывая, что Трудовой кодекс РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью работника, работодатель в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника, либо отсутствует письменное согласие работника на предоставление его персональных сведений, либо, по мнению работодателя, отсутствует угроза жизни или здоровью работника, работодатель обязан отказать в предоставлении персональных данных лицу. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных;

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

4.1.3. Предупредить лиц, получающих персональные данные работника, 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;

4.1.4. Осуществлять передачу персональных данных работника в пределах одного работодателя в соответствии с настоящим Положением;

4.1.5. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции (например, допустимо обращение за информацией о состоянии здоровья беременной женщины при решении вопроса о ее переводе на другую работу, исключающую воздействие неблагоприятных техногенных факторов);

4.1.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом и настоящим Положением, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.2. Данные требования установлены статьёй 88 Трудового кодекса РФ и не подлежат изменению, исключению, так как являются обязательными для сторон трудовых отношений,

5. Обязанности работника и работодателя

5.1. В целях обеспечения достоверности персональных данных работник обязан:

5.1.1. При приеме на работу предоставить работодателю полные и достоверные данные о себе;

5.1.2. В случае изменения сведений, составляющих персональные данные работника, незамедлительно предоставить данную информацию работодателю.

5.2. Работодатель обязан:

5.2.1. Осуществлять защиту персональных данных работника;

5.2.2. Обеспечить хранение первичной учетной документации по учету труда и его оплаты, к которой, в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов с работниками по оплате труда и др. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные;

5.2.3. Заполнение документации, содержащей персональные данные работника, осуществлять в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 05.01.04 №1;

5.2.4. По письменному заявлению работника не позднее трех дней со дня подачи этого заявления выдавать последнему копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах па другую работу, приказа об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены

надлежащим образом и предоставляться работнику безвозмездно;

5.2.5. Вести учет передачи персональных данных работника третьим лицам путем ведения соответствующего журнала, отражающего сведения о поступившем запросе (кто является отправителем запроса, дата его поступления работодателю), дату ответа на запрос, какая именно информация была передана либо отметку об отказе в ее предоставлении, либо ограничиваться помещением в личное дело работника выписок, копий документов и т.п., отражающих сведения о поступившем запросе и результатах его рассмотрения;

5.2.6. В целях обеспечения сохранности документов по личному составу увольняемых работников в случае реорганизации и ликвидации организации, а также социальной защищенности граждан, выполняющих работу по трудовому договору, включать в свои учредительные документы правила учета и сохранности документов по личному составу, а также своевременной передачи их на государственное хранение при реорганизации или ликвидации юридического лица (распоряжение Правительства РФ от 21.03.94 № 358-р «Об обеспечении сохранности документов по личному составу»);

5.2.7. В случае реорганизации или ликвидации организации учет и сохранность документов по личному составу, порядок передачи их на государственное хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами.

6. Права работников в целях защиты персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

6.1.1. Полную информацию об их персональных данных и обработке этих данных, в частности работник имеет право знать, кто и в каких целях использует или использовал его персональные данные;

6.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

6.1.3. Определение представителей для защиты своих персональных данных;

6.1.4. Доступ к относящимся к ним медицинским данным;

6.1.5. Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ и настоящего Положения. При отказе работодателя исключить или исправить персональные данные работник имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

6.1.6. 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;

6.1.7. Обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

7. Доступ к персональным данным работника

7.1. Внутренний доступ к персональным данным работника имеют:

директор;

заместитель директора по организации здравоохранения;

начальник отдела кадров, юрист;

сотрудники бухгалтерии - к тем данным, которые необходимы для выполнения конкретных функций; сам работник, носитель данных.

8. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

8.2. Неправомерный отказ работодателя исключить или исправить персональные данные работника, а также любое иное нарушение прав работника на защиту персональных данных влечет возникновение у работника права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда.

9. Сбор, обработка и защита персональных данных пациентов ОАО «МЦ «Гиппократ»

9.1 Обработка персональных данных пациентов — получение, хранение,
комбинирование, передача или любое другое использование персональных данных физического лица. Обработка персональных данных пациента осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов Российской Федерации и локальных нормативных актов Общества при осуществлении основной деятельности ОАО «МЦ «Гиппократ». Получение

9.2. Все персональные данные о пациенте работник должен получить у него самого и на основании документа, удостоверяющего личность, при этом пациент должен дать письменное согласие на использование его персональных данных по установленной в Обществе форме.

9.3. В случаях, когда работник получает необходимые персональные данные пациента у третьей стороны, должно быть его письменное согласие по установленной форме.

Примечание: Согласия пациента на получение его персональных данных от третьих лица не требуется в случаях, когда согласие пациента на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с третьим лицом. **Хранение персональных данных субъекта**

9.4. Персональные данные пациента хранятся в подразделении Общества, которое отвечает за взаимодействие с пациентом. Медицинские карты амбулаторного больного хранятся в бумажном виде в картотеке регистратуры, доступ к ним третьих лиц исключен.

Персональные данные пациента хранятся также в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные, обеспечиваются Системой защиты персональных данных и исключают доступ к ним третьих лиц.

9.5. Работник Общества, имеющий доступ к персональным данным пациентов в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные субъекта, исключающее доступ к ним третьих лиц.

  В отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные пациентов (соблюдение "политики чистых столов").

- В период отпуска, служебной командировки и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные пациентов лицу, на которое локальным актом (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

Использование (доступ, передача, комбинирование и т.д.) персональных данных пациента

9.6. Доступ к персональным данным пациента имеют работники Общества, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей. Перечень работников, допущенных к персональным данным, утверждается приказом директора Общества.

9.7. Работа в автоматизированной информационной системе (локальной компьютерной сети):

Список используемых сокращений:

АС	- автоматизированная система
Объект	- объект информатизации АС ОАО «МЦ «Гиппократ»
ОС	- операционная система
ОТСС	- основные технические средства и системы
ПЭВМ	— персональная электронно-вычислительная машина, входящая в состав ОТСС
СЗИ	- средство защиты информации
НСД	- несанкционированный доступ

9.7.1. Допуск пользователей для работы в АС осуществляется в соответствии со списком лиц, утвержденным приказом директора ОАО «МЦ «Гиппократ».

9.7.2. Присвоение пользователю прав доступа к ресурсам АС и определение возможного времени работы пользователя АС осуществляется администратором информационной безопасности АС при первичной регистрации учетной записи пользователя на ПЭВМ.

9.7.3. Учет работы пользователей АС на ПЭВМ производится средствами СЗИ от НСД, установленных на ПЭВМ, в системном журнале.

9.8. Обязанности пользователя АС:

9.8.1. Пользователь АС отвечает за правильность:

- включения и выключения ПЭВМ,
- входа в систему и все действия при работе на ПЭВМ.

Пользователь АС **обязан немедленно** сообщить администратору информационной безопасности и заместителю директора по организации здравоохранения об утрате или недостаче носителей персональных данных, амбулаторных карт, справок, ключей от защищенных помещений, хранилищ, сейфов (металлических шкафов), штампов, печатей, личных печатей. А также о других фактах, которые могут привести к разглашению персональных данных, о причинах и условиях возможной утечки сведений.

9.8.2. Время начала и окончания работы на ПЭВМ, доступ к данным и другим ресурсам фиксируются в системном журнале средствами СЗИ от НСД, установленных на ПЭВМ.

9.8.3. **Пользователь АС имеет право** в отведенное ему время решать поставленные задачи в соответствии с правами доступа к ресурсам ПЭВМ, присвоенными ему администратором информационной безопасности.

При этом для хранения файлов, содержащих конфиденциальные сведения, разрешается использовать только специально выделенные каталоги на жестком магнитном диске, а также отчуждаемые машинные носители, учтенные в установленном порядке.

9.8.4. Резервное копирование, уничтожение и восстановление информации осуществляется пользователем в рамках выделенных ему полномочий либо через администратора информационной безопасности. Пользователь АС производит резервное копирование файлов в процессе или перед окончанием работы на отчуждаемые носители, учтенные в установленном порядке.

9.8.5. При использовании отчуждаемых носителей пользователь АС каждый раз перед началом работы **с** ними обязан проверить их на отсутствие компьютерных вирусов с использованием штатных антивирусных программ, установленных на ПЭВМ, в соответствии с инструкцией по проведению антивирусного контроля. В случае обнаружения компьютерных вирусов пользователь АС обязан немедленно известить администратора информационной безопасности АС.

9.8.6. По окончании работы пользователь АС обязан выключить ПЭВМ, на которой производились работы.

9.8.7. По общим правилам хранения и передачи персональных данных **запрещается:**

-Оставлять материальные носители с персональными данными без присмотра в незапертом помещении;

- Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных;

- Сообщать персональные данные устно **или** письменно кому бы то ни было, если это не вызвано служебной необходимостью;

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а **также по письменному поручению (резолюции) вышестоящих должностных лиц.**

9.8.8. В процессе работы **пользователю запрещается:**

- без согласования с руководителем структурного подразделения или с заместителем директора по организации здравоохранения формировать и хранить базы данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные;

- запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан;

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

использовать для постоянного и временного хранения и обработки конфиденциальной информации каталоги жесткого магнитного диска не указанные в Перечне защищаемых ресурсов;

- осуществлять попытки НСД к ресурсам системы и других пользователей;

- обрабатывать информацию с ограничительной пометкой, превышающей заявленный при регистрации и разрешенный руководством ОАО «МЦ «Гиппократ»;

- пытаться подменять функции администратора информационной безопасности по перераспределению времени работы и прав доступа к ресурсам компьютера;

- покидать помещение с включенной ПЭВМ до окончания своей работы;

- разрешать другим пользователям производить в системе любые действия во время его сеанса работы;

- подключать (пытаться подключить) к ПЭВМ внешние устройства, не предусмотренные предписанием на эксплуатацию, или нарушить пломбы (печать) на корпусе ПЭВМ и других устройств, установленных на объекте;

- по окончании работы оставлять ПЭВМ включенной, оставлять в ней или на рабочем месте отчуждаемые носители или иные материалы, содержащие конфиденциальную информацию.

9.8.9. В целях предотвращения несанкционированного доступа посторонних лиц к. ресурсам пользователя осуществляется периодическая (не реже одного раза в квартал) замена личного пароля пользователя. Замена личного пароля осуществляется пользователем самостоятельно. В случае отказа системы в идентификации пользователя либо не подтверждения личного пароля пользователь АС обязан немедленно обратиться к администратору информационной безопасности АС.

9.8.10. Пользователь АС несет персональную ответственность за конфиденциальность своего пароля для входа в систему. В случае если пароль станет известным кому-либо еще кроме него пользователь АС обязан немедленно известить об этом администратора информационной безопасности АС и своего руководителя.

9.8.11. Запрещается совместное хранение конфиденциальных и не конфиденциальных (общедоступных) сведений в одном каталоге на жестком диске ПЭВМ (на одном отчуждаемом машинном носителе).

9.8.12. Затирание (обнуление, обезличивание) освобождаемых областей памяти внешних накопителей производится пользователем однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). Для затирания пользователь использует файл большего объема свободного места на внешнем носителе. Запись файла производится до полного заполнения внешнего накопителя.

9.9. В случае если Обществу оказывают услуги юридические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным пациентов, то соответствующие данные предоставляются Обществом только после подписания с ними соглашения о неразглашении конфиденциальной информации, в том числе персональных данных.

10. Организация защиты персональных данных

10.1. Защита персональных данных работника или пациента от неправомерного их использования или утраты обеспечивается Обществом.

10.2. Общую организацию защиты персональных данных лиц осуществляет администратор информационной безопасности.

10.3. Администратор информационной безопасности обеспечивает:

- ознакомление работников, которые участвуют в обработке персональных данных, под роспись с настоящим Положением;

  При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных субъекта, с данными актами также производится ознакомление работников под роспись.

- истребование с работников письменного обязательства о соблюдении конфиденциальности персональных данных пациентов и соблюдении правил их обработки;
- общий контроль соблюдения работниками Общества мер по защите персональных данных.

10.4. Организацию и контроль защиты персональных данных работников и пациентов (далее - субъектов) в структурных подразделениях Общества, работники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

10.5. Защите подлежит:

- информация о персональных данных субъекта;
- документы, содержащие персональные данные субъекта;

• персональные данные, содержащиеся на электронных носителях. 10.6. Защита сведений, хранящихся в электронных базах данных Общества, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается Системой защиты персональных данных.

11. Заключительные положения

11.1. Настоящее Положение вступает в силу с момента его утверждения директором ОАО «МЦ «Гиппократ».

11.2. Настоящее Положение доводится до сведения всех работников персонально под роспись.

11.3. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных субъектов, определяются также должностными инструкциями.

11.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

11.5. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе, работникам Общества, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Общества, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания - замечания, выговора, увольнения.

Работник Общества, имеющий доступ к персональным данным субъектов и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Обществу (пункт 7 статьи 243 Трудового кодекса РФ).

11.6. Работники Общества, имеющие доступ к персональным данным субъектов, виновные в незаконном разглашении или использовании персональных данных лиц без согласия субъектов из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со статьёй 183 Уголовного кодекса РФ.

СОГЛАСОВАНО
Администратор информационной безопасности Ермаков Е.А. Ермаков