



ПОЛОЖЕНИЕ О РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

1 Общие положения

1.1 Положение о работе с персональными данными в Краевом государственном бюджетном учреждении здравоохранения «Красноярская городская детская поликлиника №2» (далее – поликлиника) разработано в соответствии с:

- Конституцией РФ;
- Трудовым кодексом от 30.12.2001 г. № 197-ФЗ;
- Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральным законом РФ от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в РФ»;
- Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Федеральным законом от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

- иными нормативными правовыми актами, регулирующими вопросы обработки и защиты персональных данных;

- Уставом поликлиники.

1.2 Настоящим Положением определяется порядок работы (сбора, обработки, использования, распространения, хранения и т.д.) с персональными данными работников и членов семьи работников, пациентов и/или законных представителей пациентов поликлиники и гарантии конфиденциальности персональных данных.

1.3 Цель настоящего Положения:

- регламентация порядка осуществления операций с персональными данными работников и посетителей поликлиники;

- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

- обеспечение информационной безопасности поликлиники.

- установление прав и обязанностей работников поликлиники в части работы с персональными данными;

- установление механизмов ответственности работников поликлиники за нарушение локальных норм, а также положений федерального, регионального и муниципального законодательства, регулирующих использование персональных данных.

1.4 Настоящим Положением определяется порядок обработки персональных данных:

- работников поликлиники;

- пациентов и их представителей;

- лиц, ранее состоявших в трудовых отношениях с поликлиникой.

1.5 Состав персональных данных, подлежащих обработке:

- анкетные и биографические данные;

- образование;

- сведения о трудовом и общем стаже;

- паспортные данные, данные свидетельства о рождении ребенка;

- сведения о воинском учете и реквизиты документов воинского учета;

- сведения о заработной плате, доходах, имуществе и имущественных обязательствах, счетах и вкладах;

- сведения о социальных льготах;

- специальность;

- занимаемая должность;

- наличие судимостей;
- адрес регистрации и проживания;
- номера телефонов, адрес электронной почты;
- семейное и социальное положение;
- содержание трудового договора;
- государственные награды, иные награды и знаки отличия;
- содержание декларации, подаваемой в налоговую инспекцию;
- сведения, содержащиеся в документах медицинского освидетельствования;
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- полис обязательного медицинского страхования;
- данные о факте обращения пациента за оказанием медицинской помощи, сведения о состоянии его здоровья и диагнозе полученные при его медицинском обследовании и лечении;
- прочие сведения, которые могут идентифицировать личность.

1.6 Состав персональных данных, подлежащих обработке, каждой из категорий субъектов персональных данных определяется соответствующими нормативными правовыми актами.

1.7 Персональные данные содержатся в следующих документах (их копии, выписках из них):

- документы по личному составу сотрудников;
- медицинские документы пациентов;
- материалы служебных расследований, проверок;
- отчеты, направляемые в органы статистики;
- отчеты, аналитические и справочные материалы, передаваемые в государственные органы, другие учреждения;
- других делах и в информационных системах персональных данных (ИСПДн).

2. Получение и обработка персональных данных

2.1 Персональные данные поликлиника получает непосредственно от субъекта персональных данных. Получать персональные данные от третьих лиц поликлиника вправе только при наличии письменного согласия субъекта персональных данных или в иных случаях, прямо предусмотренных в законодательстве.

При запросе персональных данных субъект персональных данных должен быть предупрежден о целях, предполагаемых источниках и способах получения персональных дан-

ных, а также о характере подлежащих получению персональных данных и юридических последствиях отказа дать письменное согласие на их получение. Предупреждает субъекта об этом подразделение, на которое возложено получение персональных данных.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом.

В случаях, предусмотренных Федеральным законом, обработка персональных данных осуществляется только с согласия субъекта персональных данных, оформленного письменно по установленной настоящим Положением форме (Приложения №№ 1.1, 2). равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в установленном действующим законодательством порядке.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

2.2 Согласие на обработку персональных данных может быть отозвано субъектом персональных данных путем направления соответствующего заявления (приложение № 3).

В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований:

- обработка персональных данных осуществляется в соответствии с трудовым и пенсионным законодательством;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого или выгодоприобретателем по которому является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение его согласия невозможно;

- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с действующим законодательством сохранять врачебную тайну;

- в других случаях, предусмотренных федеральным законодательством.

2.3. Субъект персональных данных предоставляет поликлинике достоверные сведения о себе. Субъект персональных данных предъявляет документы, подтверждающие достоверность этих сведений.

Поликлиника проверяет достоверность сведений, сверяя предоставленные данные с имеющимися у субъекта персональных данных документами. Предоставление субъектом персональных данных подложных документов влечет ответственность, предусмотренную действующим законодательством.

При получении сведений, составляющих персональные данные субъектов, заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

Запрещается требовать от субъектов персональных данных документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

2.4. При изменении персональных данных субъект персональных данных письменно уведомляет поликлинику о таких изменениях в срок, не превышающий 14 дней. Субъект персональных данных предоставляет необходимые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

2.5. Поликлиника при обработке персональных данных обязана:

- осуществить блокирование персональных данных, в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора на период проверки;

- устранить допущенные нарушения в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления;

- уничтожить персональные данные в случае невозможности устранения допущенных нарушений в указанный срок;

- прекратить обработку персональных данных и уничтожить их в случае отзыва субъектом персональных данных согласия на их обработку или по достижению цели обработки в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва или с даты достижения цели обработки, если иное не предусмотрено федеральными законами.

Если цель обработки персональных данных достигнута, документы, содержащие их, должны быть уничтожены или обезличены установленным порядком.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3. Хранение персональных данных

3.1. Личные дела и личные карточки работников хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела и личные карточки работников находятся в отделе кадров в специально отведенном помещении, обеспечивающем защиту от несанкционированного доступа.

3.2. Персональные данные работников могут также храниться в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются сотрудниками отдела информационно-технического обеспечения и сообщаются индивидуально работникам, имеющим доступ к персональным данным работников.

3.3. Медицинские карты пациентов хранятся в бумажном виде в регистратурах структурных подразделений в специально отведенном помещении, обеспечивающим защиту от несанкционированного доступа.

3.4. Медицинские карты пациентов могут также храниться в электронном виде в локальной компьютерной сети и в электронных информационных системах. Доступ к электронным базам данных, содержащим персональные данные пациентов, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз

данных. Пароли устанавливаются сотрудниками отдела информационно-технического обеспечения и сообщаются индивидуально работникам, имеющим доступ к персональным данным пациентов.

3.5. В целях информационного обеспечения поликлиника может создавать общедоступные источники (сайты, служебные справочники, другие документы, в том числе электронные), содержащие персональные данные, которые включаются в эти источники с согласия субъектов персональных данных или на основании действующего законодательства.

3.6. Доступ к персональным данным работника имеют:

- главный врач;
- заместители главного врача;
- главный бухгалтер;
- руководители структурных подразделений;
- непосредственный начальник работника;

- другие работники поликлиники (бухгалтерии, отдела кадров, отдела информационно-технического обеспечения, планово-экономического отдела, организационно-правового отдела) при выполнении ими своих служебных обязанностей, допущенные к персональным данным приказом главного врача поликлиники.

Доступ к персональным данным пациентов и/или их законных представителей имеют:

- главный врач- в отношении всех пациентов и/или их законных представителей;
- заместитель главного врача по медицинской части- в отношении всех пациентов и/или их законных представителей;
- руководители структурных подразделений поликлиники- в отношении пациентов и/или их законных представителей, получающих медицинскую помощь в данном структурном подразделении;
- лечащий врач, врачи-специалисты, средний медицинский персонал- в отношении субъекта персональных данных, получающего у указанных лиц медицинскую помощь;
- заведующий отделением контроля качества медицинской помощи в отношении всех пациентов и/или их законных представителей;
- немедицинский персонал поликлиники при выполнении ими своих служебных обязанностей, связанных с оказанием медицинской помощи субъекту персональных данных, оценкой контроля качества оказанной медицинской помощи, подготовкой статистических данных, рассмотрением жалоб на действия персонала поликлиники, обслуживанием информационных систем, содержащих персональные данные пациентов и/или их законных представителей;

- сотрудники колл-центра поликлиники- в целях консультирования о порядке оказания медицинской помощи и записи на прием в поликлинику;
- сотрудники регистратур структурных подразделений- в целях консультирования о порядке оказания медицинской помощи и записи на прием в поликлинику, оформления медицинской документации, связанной с оказанием медицинской помощи субъекту персональных данных;
- сотрудники отдела информационно-технического обеспечения – в целях обслуживания информационных систем, содержащих персональные данные пациентов и/или их законных представителей;
- сотрудники отделения контроля качества медицинской помощи – при обработке персональных данных пациентов и/или их законных представителей в целях подготовки статистических данных поликлиники;
- сотрудники организационно-правового отдела (начальник отдела, специалист по связям с общественностью, юрисконсульт, секретарь) – в целях рассмотрения жалоб и обращений граждан, связанных с уставной деятельностью поликлиники, консультирования о порядке оказания медицинской помощи.

3.7. Работа с документами, содержащими персональные данные, ведется в соответствии с нормативными правовыми актами с учетом требований, предъявляемых к конфиденциальным документам. Работа с такими документами должна быть организована таким образом, чтобы исключить их просмотр посторонними (пациентами, посетителями). При оставлении рабочего места работником и по окончании рабочего дня документы должны убираться в запирающиеся шкафы (сейфы, картотеки).

4. Использование персональных данных

4.1. Персональные данные работника и членов его семьи используются в целях, связанных с выполнением работником трудовых функций. Поликлиника использует персональные данные работника, в частности, для решения вопросов о приеме на работу, о продвижения работника по службе, обучении и повышения квалификации работника, очередности предоставления ежегодного отпуска, установления размера заработной платы и т.д. На основании персональных данных работника решается вопрос о допуске его к информации, составляющей служебную или коммерческую тайну, о допуске к тем или иным видам медицинской деятельности.

4.2. Персональные данные пациентов, законных представителей пациентов используются в целях оказания пациенту медицинской помощи. Поликлиника использует персо-

нальные данные пациентов и/или законных представителей пациентов, в частности, в целях записи на прием в поликлинику, сбора анамнеза пациента, назначения и контроля эффективности лечения, контроля качества оказанной медицинской помощи, оформления медицинской документации и т.д.

5. Передача и распространение персональных данных

5.1. При передаче поликлиникой персональных данных субъект персональных данных должен дать на это согласие в письменной или электронной форме. Если субъект персональных данных оформил согласие на передачу персональных данных в электронной форме, то он подписывает согласие усиленной электронной цифровой подписью.

5.2. Поликлиника вправе передать информацию, которая относится к персональным данным субъекта персональных данных без его согласия, если такие сведения нужно передать по запросу государственных органов, в порядке, установленном федеральным законом.

5.3. Поликлиника не вправе предоставлять персональные данные субъекта персональных данных третьей стороне без его письменного согласия за исключением случаев, установленных федеральным законом.

5.4. Основанием для рассмотрения возможности и целесообразности передачи персональных данных третьей стороне является письменный запрос (мотивированное ходатайство) на имя главного врача, в котором должно быть указано:

- состав запрашиваемых сведений;
- обоснование необходимости работы с этими сведениями;
- форма передачи сведений: доступ (ознакомление, выписки или копирование) или предоставление (в каком виде: электронном или бумажном);
- представитель, уполномоченный на получение персональных данных (фамилия, имя, отчество, серия и номер паспорта, когда и кем они выданы);
- обязательство соблюдать режим конфиденциальности полученных данных.

Передача персональных данных возлагается на подразделения, ответственные за их обработку.

Подразделения, ответственные за передачу, отправку и регистрацию персональных данных, ведут журнал учета выдачи персональных данных (Приложение № 4).

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Запрещается:

- передавать кому-либо персональные данные по телефону;
- сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

5.4. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение информации, относящейся к персональным данным субъекта персональных данных, поликлиника обязана отказать лицу в выдаче информации. Лицу, обратившемуся с запросом, выдается уведомление об отказе в выдаче информации.

5.5. Персональные данные работника могут быть переданы представителям работников в порядке, установленном Трудовым кодексом, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

5.6. Поликлиника не вправе распространять персональные данные субъекта персональных данных третьим лицам без согласия субъекта на передачу таких данных.

5.7. Согласие на обработку персональных данных, разрешенных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных (Приложение № 1.2.).

5.8. Поликлиника обязана обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на распространение персональных данных.

5.9. В случае если из предоставленного согласия на распространение персональных данных не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются поликлиникой без права распространения.

5.10. В случае, если из предоставленного согласия на передачу персональных данных не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных или не указал категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, поликлиника обрабатывает такие персональные данные без возможности передачи (распространения, предоставления, доступа) неограниченному кругу лиц.

5.11. Согласие на распространение персональных данных может быть предоставлено поликлинике:

- непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

5.12. В согласии на распространение персональных данных субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ поликлиники в установлении субъектом данных запретов и условий не допускается.

5.13. Поликлиника обязана в срок не позднее трех рабочих дней с момента получения согласия субъекта на распространение персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных для распространения.

5.14. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по его требованию. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению.

5.15. Действие согласия субъекта персональных данных на распространение персональных данных, прекращается с момента поступления поликлинике требования, указанного в пункте 5.14 настоящего положения.

5.16. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона от 27.07.2006 № 152-ФЗ или обратиться с таким требованием в суд. Поликлиника или третье лицо обязаны прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования или в срок, указанный во вступившем в законную силу решении суда. Если такой срок в решении суда не указан, то поликлиника или третье лицо обязано прекратить передачу персональных данных субъекта в течение трех рабочих дней с момента вступления решения суда в законную силу.

6. Права и обязанности субъекта персональных данных

6.1. В целях защиты персональных данных, обрабатываемых поликлиникой, субъект персональных данных имеет право:

- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

- требовать уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для поликлиники персональных данных;

- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

- определять своих представителей для защиты своих персональных данных;

- на сохранение и защиту своей личной, семейной и врачебной тайны;

- требовать извещения поликлиникой всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжаловать неправомерные действия или бездействие поликлиники при обработке и защите персональных данных.

6.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных поликлиникой;

- правовые основания и цели обработки персональных данных;

- цели и применяемые поликлиникой способы обработки персональных данных;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством;

- иные сведения, предусмотренные федеральным законодательством.

6.3. Субъект персональных данных обязан:

- передавать поликлинике комплект достоверных документированных персональных данных, состав которых установлен действующим законодательством РФ;

- предоставить поликлинике полные достоверные данные о себе;

- своевременно сообщать поликлинике об изменении своих персональных данных.

6.4. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

7. Гарантии конфиденциальности персональных данных

7.1. Информация, относящаяся к персональным данным субъекта, является конфиденциальной и охраняется законом.

7.2. Субъект персональных данных вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

7.3. В случае разглашения персональных данных без согласия субъекта он вправе требовать от поликлиники разъяснений.

7.4. Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;
- по истечении срока их хранения;
- в других случаях, предусмотренных федеральным законодательством.

8. Организация защиты информации

8.1. Мероприятия по защите информации являются составной частью управленческой и производственной деятельности и проводятся в рамках единой комплексной системы защиты информации поликлиники.

8.2. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

8.3. Организационные меры предусматривают организацию и контроль доступа в контролируемую зону (медицинские, административные корпуса), к объектам информатизации, их физическую защиту, охрану, в том числе техническими средствами и системой видеонаблюдения, режим работы на них, разграничение прав доступа к информационным ресурсам, порядок хранения, применения, передачи и уничтожения информации, другие меры. Эти меры вводятся организационно-распорядительными и другими документами.

8.4. Объектами, подлежащими защите в поликлинике, являются:

- информационные ресурсы: конфиденциальная и открытая важная (ценная) информация на бумажных и машинных носителях информации, а также речевая информация;

- технические средства обработки и передачи информации: средства вычислительной техники (СВТ), автоматизированные системы (АС), вычислительные сети (ВС), аппаратное и программное обеспечение этих систем, линии и средства связи, посредством которых передается конфиденциальная и другая информация, другие средства обработки и передачи информации;

- защищаемые помещения.

8.5. Защита информации в информационной среде поликлиники основывается на выявлении, оценке и противодействии возможным угрозам безопасности информации.

8.6. Основными видами угроз безопасности информации являются:

- противоправные действия внешних и внутренних нарушителей;
- ошибочные действия пользователей и обслуживающего персонала;
- отказы и сбои технических средств;
- вредоносные программные воздействия на информацию и средства информатизации, приводящие к ее модификации, блокированию, уничтожению или копированию, а также нарушению правил эксплуатации средств вычислительной техники, вычислительных сетей и автоматизированных систем.

8.7. Меры по технической и криптографической защите информации включают использование программных, программно-аппаратных, аппаратных и криптографических средств для защиты информации в информационных системах.

8.8. Общее и методическое руководство разработкой и организацией мероприятий по защите информации, их нормативное обеспечение и контроль за эффективностью предусмотренных мер возлагается на организационно-правовой отдел и отдел по информационно-техническому обеспечению (далее – ОПО, ОИТО).

8.9. Обеспечение защиты информации в автоматизированных системах, вычислительных сетях и других объектах информатизации возлагается на руководителей структурных подразделений и сотрудников; на других сотрудников, специалистов (администраторы АС, сетевые администраторы и др.).

8.10. Все мероприятия по разработке, созданию и модернизации объектов информатизации, изменению состава и конфигурации программных и технических средств, обрабатывающих конфиденциальную информацию, все мероприятия и изменения в организационно-технических решениях по защите информации, а также все разрабатываемые документы касающиеся защиты информации должны быть согласованы с отделами, указанными в п.8.8.

8.11. Обязанности по защите персональных данных руководителей структурных подразделений и сотрудников определяются настоящим Положением (Приложения №№ 5, 6), должностными инструкциями, положением о подразделении и другими нормативными и организационными документами поликлиники.

8.12. Документы по защите персональных данных, доводятся под подпись до всех сотрудников в соответствии с занимаемой должностью при трудоустройстве на работу.

8.13. Руководители структурных подразделений проводят инструктаж по защите персональных данных с сотрудниками на рабочем месте один раз в год (в начале года), внеплановый — по необходимости под роспись в журнале ознакомления (Приложение № 7).

8.14. Запрещается допускать к работе лиц, не изучивших требования документов по защите персональных данных.

8.15. При прекращении трудовых отношений с поликлиникой работник обязан сдать все материальные носители сведений, содержащих персональные и конфиденциальные данные работников и пациентов, а также ключи от помещений и шкафов, в которых они хранятся.

8.16. Защита информации в процессе ведения делопроизводства и служебной переписки обеспечивается точным соблюдением требований нормативных документов, регламентирующих ведение делопроизводства.

9 Организационно-технические мероприятия по защите информации

9.1. Определение необходимых организационно-технических мероприятий по защите информации проводится на основании нормативных правовых и методических документов, регламентирующих защиту информации.

9.2. Безопасность информации на необходимом уровне обеспечивается точным выполнением правил эксплуатации технических и программных средств обработки и передачи информации, технологии обработки информации, требований по защите информации и ведению делопроизводства, а также организационно-техническими мероприятиями по защите информации.

9.3. Организационные меры направляются на исключение или существенное затруднение несанкционированного доступа в защищаемые помещения, к техническим средствам обработки информации и информационным ресурсам. Это достигается организацией на территории поликлиники, средствами видеонаблюдения, физической защитой и режимом разграничения доступа к ним.

9.4. Защищаемые помещения должны размещаться в пределах контролируемой зоны, должны быть оборудованы средствами охранно-пожарной сигнализации, быть в зоне видеонаблюдения.

9.5. Физическая защита защищаемых помещений должна исключить несанкционированный доступ в них, нарушение работоспособности и хищение технических средств обработки, хранения и передачи информации, а также самой информации. Это обеспечивается оборудованием входных дверей надежными замками, в том числе электронными или механическими кодовыми, механизмами, минимизирующими возможность случайного оставления их открытыми (доводчики закрытия дверей и т. п.), и другими необходимыми мерами.

9.6. В защищаемом помещении должен быть установлен режим доступа и работы, обеспечивающий безопасность информации. Технические средства обработки информации должны быть закреплены за конкретными работниками. Печатающие устройства, видеотерминалы, графопостроители, а также конфиденциальные документы должны размещаться так, чтобы исключался визуальный просмотр информации посторонними лицами (пациентами, посетителями), при необходимости должны применяться дополнительные меры, исключающие подобный просмотр (шторы, жалюзи, и т. п.).

9.7. Порядок сдачи защищаемого помещения под охрану и снятия с охраны определяется локальными нормативными актами и инструкциями поликлиники.

9.8. Все технические, ремонтные, строительные, хозяйственные и другие работы в защищаемом помещении должны выполняться с разрешения (распоряжения) руководителя подразделения и под контролем ответственного за помещение.

9.9. На защищаемое помещение руководитель подразделения составляет Технический паспорт (Приложение № 11).

9.10. Запрещается проведение любых мероприятий и работ с использованием сведений конфиденциального характера без принятия необходимых мер защиты информации.

9.11. Защита информации, обрабатываемой с использованием АС, СВТ, ВС, является составной частью работ по созданию и эксплуатации этих средств, должна осуществляться в виде системы (подсистемы) защиты информации и предусматривать комплекс организационных, технических (аппаратных, программных, аппаратно-программных) и криптографических средств, и мер при ее автоматизированной обработке, хранении и передаче по каналам связи, направленных на решение следующих основных задач:

- предотвращение НСД к информации с целью ее хищения, уничтожения, модификации, блокирования, утечки, копирования;
- предотвращение специальных программно-технических воздействий, вызывающих уничтожение, модификацию, блокирование информации или сбои в работе СВТ;

- исключение утраты (повреждения) информации при технических сбоях, ошибках пользователей и других нештатных ситуациях.

9.12. Организационно-технические мероприятия по защите информации выполняются на всех этапах жизненного цикла АС и других объектов информатизации.

9.13. СВТ и программные средства, применяемые для обработки конфиденциальной информации, а также применяемые средства защиты информации должны быть сертифицированы.

9.14. Предотвращение НСД к информации обеспечивается разграничением и управлением доступа пользователей к ресурсам информационных систем, применением специальных программно-аппаратных средств защиты, использованием криптографических средств защиты информации и организационными мероприятиями.

9.15. Разграничение доступа пользователей к ресурсам информационных систем реализуется конфигурированием и настройкой сетевого оборудования, межсетевых экранов, созданием матриц доступа пользователей к серверам и рабочим станциям и их ресурсам, установкой соответствующих разрешений в настройках операционных систем, другими мерами и средствами.

9.16. Управление доступом подразумевает управление идентификацией и аутентификацией пользователей, управление присвоением им прав и привилегий по доступу к ресурсам, контроль доступа и выявление попыток НСД.

9.17. Идентификация и аутентификация пользователей обеспечивается использованием уникальных имени пользователя (идентификатора) и пароля.

9.18. Парольная защита при работе на СВТ, в АС и ВС осуществляется с целью предотвращения несанкционированного доступа (НСД) к информации, она является составной частью подсистемы управления доступом общей системы защиты от НСД.

9.19. Вход в операционные системы ПЭВМ, другие СВТ, ВС, АС должен быть ограничен паролем. Конфиденциальная информация должна храниться в ПЭВМ только в базах и банках данных, папках и файлах, вход в которые ограничен паролем.

Ответственность за организацию системы парольной защиты несут:

- в подразделении – руководитель подразделения;
- в автоматизированной системе – администратор;
- на АРМ – пользователь.

Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы (ПЭВМ) самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из шести символов, а для административных учетных записей не менее десяти, большее количество символов повышает его надежность;
- пароль обязательно должен состоять из букв и цифр, использование букв в верхнем и нижнем регистрах и специальные символы (@, #, \$, &, *, % и т.п.) повышают его надежность;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. п.).
- новый пароль пользователя не должен совпадать с именем учетной записи пользователя и с предыдущими паролями, должен отличаться от старого не менее чем в шести позициях.

Пароли пользователей на доступ к различным ресурсам (для входа в операционную систему ПЭВМ, информационную систему, базы данных, электронной почты и др.) должны быть различными.

При вводе пароля необходимо исключить возможность его видеть посторонними лицами (другими работниками, посетителями).

Запрещается включать пароли в какой-либо автоматизированный процесс начала сеанса.

Пользователь обязан сохранять в тайне свой пароль, не сообщать его другим лицам.

Смена паролей должна проводиться в случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) или в случае компрометации пароля (если он стал известен другим лицам или есть подозрение об этом).

Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

9.20. Запрещается подключение АС, ВС и отдельных ПЭВМ, обрабатывающих конфиденциальную информацию, к сети Интернет и к другим информационным системам и сетям без использования специальных сертифицированных технических и криптографических средств защиты информации.

9.21. Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи или предназначенные для этого криптографические средства защиты информации.

9.22. Служебный электронный документооборот со сведениями, не составляющими конфиденциальную информацию, должен вестись только с ящиков электронной почты, зарегистрированных в домене поликлиники.

9.23. Обмен конфиденциальной информацией между отдельными автоматизированными рабочими местами (АРМ) может осуществляться с помощью съемных носителей информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации. При этом должны соблюдаться меры безопасности: носители должны быть учтены и храниться установленным порядком, информация должна пройти антивирусный контроль, должна быть закрыта паролем и др.

9.24. Предотвращение вредоносных программно-математических воздействий, вызывающих уничтожение, искажение информации или сбои в работе средств информатизации, обеспечивается применением специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), средств криптографической защиты информации, контролем целостности программной среды АС и СВТ, постоянным антивирусным контролем.

9.25. Для повышения надежности сохранности информации, хранящейся в электронных базах данных, для восстановления информации в случаях ее утраты (повреждения) организуется резервное копирование и архивирование. Резервные копии информации целесообразно хранить на различных носителях и в разных местах, они должны быть закрыты паролем. Порядок и сроки резервирования, архивирования, хранения и восстановления информации в автоматизированных и других системах определяется регламентом системы; в подразделении этот порядок определяет руководитель подразделения.

9.26. Электропитание средств информатизации целесообразно осуществлять через развязывающие фильтры и с использованием источников бесперебойного питания. Серверы, активное сетевое оборудование, а также наиболее важные рабочие станции целесообразно обеспечивать резервными линиями электропитания, автономными источниками резервного электропитания.

9.27. Для защиты речевой информации при ведении конфиденциальных переговоров, совещаний, предотвращения утечки информации в акустическом канале целесообразно принимать меры по ограничению допуска к объектам защиты, повышению их звукоизоляции, проводить проверки на наличие закладочных устройств несанкционированного прослушивания (радиомикрофоны, диктофоны и другие технические средства).

9.28. Использование мобильных электронных устройств при проведении служебных совещаний, собраний, и других массовых мероприятий в помещениях поликлиники допускается только с разрешения руководителя подразделения или проводимого мероприятия. Руководитель, проводящий мероприятие, обязан предупредить присутствующих об отключении мобильных средств связи, а при необходимости и других устройств.

10 Организация контроля в подразделениях

10.1. Контроль выполнения требований по защите, эффективности предусмотренных мер защиты информации является процедурой (составной частью) процесса защиты информации.

10.2. Задачи контроля:

- проверка соответствия мероприятий по защите информации требованиям федеральных нормативных правовых и локальных нормативных актов;
- оценка обоснованности принятых мер защиты;
- проверка своевременности и полноты выполнения требований руководящих документов, регламентирующих организацию и порядок осуществления мероприятий по защите информации;
- оценка эффективности предусмотренных мер защиты информации.

10.3. Осуществляются следующие виды контроля:

- постоянно - руководителями структурных подразделений;
- периодически - отделом ИТО, другими лицами в соответствии с функциональными обязанностями;
- плановый - отделом ИТО и специально назначенными комиссиями в соответствии с планом контроля, а также перед вводом технических и программных средств в эксплуатацию;
- внеплановый - специально назначенной комиссией (должностным лицом, группой) по распоряжению главного врача.

10.4. Контроль может проводиться как с уведомлением руководителя проверяемого объекта, так и без уведомления.

10.5. По результатам контроля дается оценка состояния работ и эффективности, принятых мер защиты информации. Защита информации считается эффективной, если принимаемые меры обеспечивают реализацию заданных целей, замыслов, требований и соответствуют установленным нормам. Результаты контроля отражаются в актах, справках, докладах.

10.6 Допуск лиц к проведению контроля за состоянием защиты информации производится на основании приказа или распоряжения главного врача.

11 Ответственность за нарушение защиты персональных данных субъекта

11.1. Руководители подразделений и сотрудники, ведущие обработку персональных данных, на которых возложено сопровождение и администрирование ИСПДн, несут персональную ответственность за организацию обработки персональных данных и их защиты.

11.2. Лицо, ведущее обработку персональных данных, обязано знать и выполнять установленные требования по обработке и защите персональных данных, не разглашать их.

11.3. Разглашение персональных данных (передача их посторонним лицам, в том числе, сотрудникам администрации, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъектов, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарной ответственности.

11.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных и конфиденциальных данных субъекта, привлекаются к 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.

12. Заключительные положения

12.1. Положение пересматривается в случае возникновения несоответствий с нормативными правовыми актами РФ, по мере совершенствования программно-технического обеспечения и информационных технологий в поликлинике.

12.2. Положение вступает в силу с момента утверждения главным врачом.

12.3. Все сотрудники поликлиники должны быть ознакомлены под подпись с Положением и изменениями к нему.

12.4. Положение размещается на официальном сайте поликлиники с целью ознакомления с ним субъектов персональных данных и их представителей.

Приложение № 1.1
Форма заявления (для работника)

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество субъекта)
зарегистрированный (-ая) по адресу: _____
имеющий (-ая) документ, удостоверяющий личность: _____
(наименование документа, номер, серия, дата выдачи документа, кем выдан)

в соответствии с п. 4 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» в целях исполнения определёнными сторонами условий трудового договора даю согласие КБУЗ «Красноярской городской детской поликлинике № 2», расположенной по адресу: г.Красноярск, ул. Матросова, 7а (далее - Оператор) на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных и персональных данных членов моей семьи, а именно: на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление, доступ, обезличивание, блокирование, удаление, уничтожение персональных данных, а также на передачу такой информации третьим лицам, если это необходимо в случаях, установленных нормативными документами вышестоящих органов и законодательством.

Перечень персональных данных, передаваемых на обработку:

- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- гражданство;
- знание иностранного языка;
- образование и повышение квалификации или наличие специальных знаний;
- профессия, специальность;
- сведения о трудовом стаже, сведения о приёмах, переводах, перемещениях и увольнениях по предыдущим местам работы, размер заработной платы;
- состояние в браке, состав семьи, место работы или учёбы членов семьи и родственников;
- паспортные данные, адрес места жительства, дата регистрации по месту жительства;
- номер телефона;
- идентификационный номер;
- номер страхового свидетельства государственного пенсионного страхования;
- сведения, включённые в трудовую книжку;
- сведения о воинском учёте;
- фотография;
- сведения о состоянии здоровья, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям.

Я ознакомлен (а) с документами о персональных данных КБУЗ «Красноярская городская детская поликлиника № 2», устанавливающими порядок обработки персональных данных, а так же со своими правами и обязанностями в этой области.

Я оставляю за собой право отозвать свое согласие на обработку персональных данных посредством составления соответствующего письменного заявления.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме, далее в течение срока хранения личного дела субъекта.

(подпись, Ф.И.О. работника)

«____» _____ 20__ г.

Приложение № 1.2.
Форма заявления (для работника)

**Согласие на обработку персональных данных,
разрешенных субъектом персональных данных для распространения**

Я, _____, паспорт серии _____ № _____, выдан
«__» _____ г. _____,

Зарегистрированный (ая) по адресу: _____,
руководствуясь статьей 10.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", заявляю о согласии на распространение КГБУЗ «Красноярская городская детская поликлиника № 2» (г. Красноярск, ул. Королева, 3а) моих персональных данных с целью размещения информации обо мне на информационных ресурсах КГБУЗ «Красноярская городская детская поликлиника №2 в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да / нет)	Неограниченно-му кругу лиц (да / нет)	Условия и запреты	Дополнительные условия
персональные данные	фамилия				
	имя				
	отчество				
	дата				
	месяц				
	год рождения				
	место рождения				
	адрес				
	семейное положение				
	образование				
	профессия				
	Мобильный телефон				
...					
Биометрические персональные данные	Цветное цифровое фотографическое изображение лица				
	Видео				

Окончание приложения № 1.2

Сведения об информационных ресурсах Оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
https: гдп2.рф	Предоставление сведений неограниченному кругу лиц
Инстаграмм @kgdp_2	Предоставление сведений неограниченному кругу лиц

Настоящее согласие дано мной добровольно и действует с даты подписания и заканчивается в связи с моим увольнением.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

«___» _____ 2021 г. _____

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество субъекта)

зарегистрированный (-ая) по адресу: _____

имеющий (-ая) документ, удостоверяющий личность: _____

(наименование документа, номер, серия, дата выдачи документа, кем выдан)

как законный представитель на основании свидетельства о рождении _____

(номер, серия, дата выдачи документа, кем выдан)

в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» в целях оказания медицинской помощи даю согласие КБУЗ «Красноярской городской детской поликлинике № 2», расположенной по адресу: г.Красноярск, ул. Матросова, 7а (далее - Оператор) на обработку моих персональных данных и персональных данных моего ребенка _____

(Фамилия, Имя, Отчество, дата рождения)

к которым относятся:

- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- состояние в браке, состав семьи, место работы или учёбы членов семьи и родственников;
- паспортные данные, адрес места жительства, дата регистрации по месту жительства;
- номер телефона;
- номер полиса обязательного медицинского страхования;
- номер страхового свидетельства государственного пенсионного страхования;
- сведения о состоянии здоровья, заболеваниях.

Оператор имеет право на включение в списки (электронные реестры) и обмен (прием и передачу) моих персональных данных и данных моего ребенка со страховыми и медицинскими организациями, связанными договорными обязательствами с Оператором, с использованием машинных носителей или по каналам связи, с использованием шифровальных (криптографических) средств, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка осуществляется лицом, обязанным сохранять профессиональную тайну.

Оператор вправе обрабатывать мои персональные данные и данные моего ребенка для получения государственной и оперативной статистической отчетности, включая сбор, накопление, хранение, обновление, изменение, систематизацию, использование, обезличивание, блокирование, уничтожение.

Окончание приложения № 2

Передача моих персональных данных и данных моего ребенка иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Я оставляю за собой право отозвать свое согласие на обработку персональных данных посредством составления соответствующего письменного заявления.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

(подпись субъекта персональных данных или его законного представителя)

«____» _____ 20__ г.

Приложение № 3
Форма заявления

Главному врачу КБУЗ «КГДП №2»

Ф.И.О.

от _____
Ф.И.О. субъекта персональных данных

Адрес, где зарегистрирован субъект

Паспорт, номер, серия, дата выдачи, кем выдан

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с неправомерным их использованием.

О прекращении обработки моих персональных данных прошу уведомить меня в письменной форме.

(подпись)

(расшифровка подписи)

« ____ » _____ 20 ____ г.

Приложение № 4

Форма журнала учета выдачи персональных данных

Журнал учета выдачи персональных данных

Регистрационный номер	Дата, номер запроса (мотивированного ходатайства)	Сведения об организации (лице), направившей запрос	Дата, исх. номер ответа на запрос о передаче персональных данных	Какая информация передана (по каким причинам дан отказ в предоставлении персональных данных)	Кто получил данные (фамилия, инициалы, номер паспорта, когда и кем он выдан)	Примечание
1	2	3	4	5	6	7

Инструкция по защите информации руководителю структурного подразделения

Руководитель структурного подразделения отвечает за организацию и проведение необходимых мероприятий по защите информации в подразделении и выполнение всех требований нормативных документов по защите информации работниками подразделения.

Руководитель подразделения обязан:

1. Знать и строго выполнять требования локальных нормативных актов, других документов по защите информации; во взаимодействии с организационно-правовым отделом и отделом информационно-технического обеспечения отделом организовать и обеспечить функционирование системы защиты информации подразделения; все разрабатываемые документы, касающиеся вопросов защиты информации, согласовывать с организационно-правовым отделом.

2. Контролировать выполнение работниками подразделения требований по защите информации.

3. Участвовать в подготовке необходимых документов об организации защиты конфиденциальной информации в подразделении; в дальнейшем при изменениях в организационной и инфраструктуре, кадровых изменениях своевременно вносить изменения в эти документы.

4. Допускать к работе с конфиденциальной информацией, необходимой для исполнения служебных обязанностей, работников, изучивших требования нормативных документов по защите информации, в соответствии со Списком (Приложение № 8).

5. Организовать и поддерживать в подразделении режим допуска в защищаемые помещения, к техническим средствам обработки информации и к информационным ресурсам. Оформлять Технические паспорта на защищаемые помещения, своевременно вносить в них изменения.

6. Закреплять за работниками подразделения автоматизированные рабочие места, средства вычислительной техники и другие технические средства обработки и передачи информации.

7. Допускать работников к исполнению служебных обязанностей только после изучения ими Положения о персональных данных и других документов по защите информации, в дальнейшем документы доводить не реже одного раза в год.

8. Определять работникам задачи и обязанности, организовать проведение инструктажей и занятий с ними по вопросам защиты информации, прививать им правила и нормы служебной этики, направленные на обеспечение информационной безопасности.

9. Принимать меры по предотвращению случаев разглашения (утечки) конфиденциальной информации и утраты документов, проводить постоянную работу по выявлению возможных каналов утечки информации и их закрытию, по совершенствованию системы защиты информации.

10. Определять порядок использования мобильных электронных устройств в ЗП, при проведении служебных совещаний, конференций, собраний и других массовых мероприятий с учетом требований настоящего Положения. Перед проведением мероприятий требовать от присутствующих отключать средства мобильной связи, а в случае необходимости и другие устройства.

Окончание приложения № 5

11. Организовать и поддерживать систему парольной защиты информации в средствах вычислительной техники.

12. Организовать резервное копирование и архивирование конфиденциальной и открытой ценной (важной) информации.

13. Согласовывать проведение работ по созданию, модернизации и внедрению объектов информатизации, а также все проводимые мероприятия и принимаемые меры по защите информации с организационно-правовым отделом и отделом информационно-технического обеспечения.

14. В случае нарушения технологии обработки конфиденциальной информации, обнаружения утечки или предпосылок к утечке конфиденциальной информации и несанкционированного доступа к ней информировать об этом отдел информационно-технического обеспечения, принимать меры по их пресечению.

15. Предоставлять сотрудникам отдела информационно-технического обеспечения запрашиваемую информацию, беспрепятственно допускать их к объектам информатизации и информационным ресурсам подразделения в соответствии с их должностными обязанностями и полномочиями.

За нарушение требований настоящей инструкции руководитель несет ответственность в соответствии с действующим законодательством Российской Федерации.

Инструкция по защите информации работнику поликлиники

Работник обязан:

1. Знать и строго выполнять требования по эксплуатации технических средств, вверенных ему в пользование, нормативных документов по ведению делопроизводства, технологии обработки (передачи) и защиты информации.

2. Работать только с теми служебными документами и сведениями, а также техническими средствами, к которым он получил доступ в силу своих служебных обязанностей.

3. Не разглашать ставшую известной ему по службе или иным путем конфиденциальную информацию поликлиники.

4. Обеспечить сохранность доверенных ему по службе документов, как на бумажной основе, так и машинных носителей информации (флэш-накопители, внешние накопители на жестких дисках, компакт-диски, иные устройства, фото-, кино-, видео- и аудиопленки, и др.), вести их учет и хранение в установленном порядке.

5. Соблюдать требования по парольной защите при работе на средствах вычислительной техники.

6. Содержать на рабочем месте мониторы, печатающие устройства, а также конфиденциальные документы таким образом, чтобы исключить визуальный просмотр информации посторонними (посетителями, пациентами и т.д.).

7. Перед началом работы на ПЭВМ проверять наличие и работоспособность антивирусных программ, следить за их своевременным обновлением. Все электронные носители информации перед их применением проверять на наличие вирусов.

8. Оставляя рабочее место независимо от времени, активизировать временную блокировку экрана монитора и клавиатуры ПЭВМ.

9. Ставить в известность руководителя подразделения и сетевого администратора (администратора АС) обо всех подозрительных ситуациях (нарушение функционирования средств вычислительной техники, АС, изменение конфигурации программного обеспечения, наличие вируса и т. п.).

10. Передавать служебные документы только своему руководителю, адресату, или другим лицам по указанию своего руководителя.

11. Служебный электронный документооборот вести только с ящиков электронной почты, зарегистрированных в домене поликлиники.

12. По согласованию с руководителем подразделения установленным порядком создавать и хранить резервные копии конфиденциальной и открытой ценной (важной) информации.

13. Пресекать действия посторонних лиц (посетителей) и других работников, направленные на разглашение конфиденциальной информации, создание предпосылок к нарушению ее безопасности, а также на несанкционированный доступ к доверенной ему служебной информации, требовать от них соблюдения установленного порядка в служебном помещении. В случае невыполнения этих требований сообщать своему руководителю.

14. Не выносить из служебного помещения конфиденциальные документы и другие носители конфиденциальной информации без разрешения (распоряжения) своего руководителя.

15. Не допускать без разрешения (распоряжения) своего руководителя к работе на технических средствах (вычислительная и оргтехника, средства связи и др.), а также к контрольно-техническим, ремонтно-строительным и другим работам в служебном помещении посторонних (посетителей, работников не своего подразделения).

16. Не оставлять в служебном помещении при выходе из него посторонних (посетителей, пациентов и т.д.) одних, а конфиденциальные документы – доступными для других работников и посторонних (посетителей, пациентов и т.д.).

17. Никому не сообщать конфиденциальную информацию по телефону, факсу, электронной почте.

18. Не устанавливать, не удалять, не копировать, не переименовывать программное обеспечение без согласования с руководителем своего подразделения и системным администратором.

19. Не сообщать свои пароли и идентификаторы другим лицам, хранить их записанными только в местах, недоступных для других.

20. Использовать мобильные электронные устройства (ноутбук, блокнотный, планшетный, портативный компьютер, личный цифровой помощник (персональный цифровой секретарь), радиоприемники, радиопередатчики, средства аудио, фото, видеозаписи, средства мобильной связи и др.) при проведении служебных совещаний, конференций, собраний, и других массовых мероприятий в помещениях поликлиники только с разрешения руководителя подразделения или проводимого мероприятия. Перед проведением мероприятий указанные средства отключать.

За нарушение требований настоящей инструкции работник несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 7

Форма журнала доведения до работников
документов по защите информации

ЖУРНАЛ
доведения до работников документов по защите информации

(наименование подразделения)

№ п/п	Название документа, его реквизиты (дата, номер)	Кто и когда ознакомлен с документом				Примечание
		Фамилия, инициалы	Должность	Подпись	Дата	
1	2	3	4	5	6	7

Приложение № 8

Форма списка работников

Список работников

_____,
(наименование подразделения)

допущенных к работе с конфиденциальной информацией поликлиники

№ п/п	Должность	Фамилия, инициалы	Информация, к которой допущен работник (индекс дел в номенклатуре)	Права	Примечание
1	2	3	4	5	6

Примечание. Список утверждается приказом (распоряжением) главного врача

Приложение № 9

Форма списка защищаемых помещений

Список защищаемых помещений

(наименование подразделения)

№ п/п	Номер помещения	Назначение помещения	Ответственный за помещение	Рабочий телефон	Примечание
1	2	3	4	5	6

Примечание. Список утверждается приказом (распоряжением) главного врача**Приложение № 10**

Форма списка информационных ресурсов

Список информационных ресурсов

(наименование подразделения)

содержащих конфиденциальную информацию поликлиники

№ п/п	Наименование ресурса (дело, документ, база данных)	Индекс дела	Количество дел (АРМ)	Место нахождения	Примечание
1	2	3	4	5	6

Примечание. Список утверждается приказом (распоряжением) главного врача

ТЕХНИЧЕСКИЙ ПАСПОРТ
на защищаемое помещение № ____

Назначение помещения

Наименование подразделения

Адрес подразделения

Должность руководителя подразделения

Подпись, инициалы, фамилия руководителя подразделения

«Ознакомлен»
Ответственный за помещение

Подпись, инициалы, фамилия

20_ г.

Инструкция
по обеспечению режима безопасности и эксплуатации
оборудования, установленного в защищаемом помещении № _____

1. Ответственность за режим допуска и безопасности в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет ответственный за защищаемое помещение _____

(должность, фамилия, инициалы ответственного)

2. Установка нового оборудования, мебели и т. п., замена их, а также ремонт помещения и другие работы в нем должны проводиться только по согласованию с руководителем подразделения и в присутствии работников, имеющих допуск в защищаемое помещение. Запрещается установка и модернизация технических средств хранения, обработки и передачи информации без согласования с _____

(должность руководителя подразделения)

3. В нерабочее время, а также при отсутствии работников, имеющих допуск в защищаемое помещение, оно должно закрываться на ключ. Выдача ключей от помещения осуществляется под роспись в журнале выдачи. Уборка в помещении должна производиться в присутствии работников, имеющих допуск в это защищаемое помещение. По окончании работ назначенный руководителем подразделения работник обязан закрыть помещение на ключ.

4. При проведении конфиденциальных мероприятий и работ запрещается присутствие в помещении посторонних лиц; не рекомендуется использовать средства мобильной и других видов связи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком и спикерфоном рекомендуется отключать эти аппараты.

5. Должны строго выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении.

6. Использовать мобильные электронные устройства (ноутбук, блокнотный, планшетный компьютер, портативный миникомпьютер, личный цифровой помощник (персональный цифровой секретарь), радиоприемник, средства аудио, фото, видеозаписи и другие устройства) при проведении конфиденциальных мероприятий и работ, собраний и других мероприятий только с разрешения руководителя подразделения. Средства мобильной связи перед указанными мероприятиями отключать.

7. За эксплуатацию и правильное использование технических средств на АРМ несет ответственность пользователь этого АРМ, а технических средств коллективного пользования – лицо, назначенное руководителем подразделения.

8. Контроль за выполнением установленного режима безопасности и эксплуатации помещения осуществляют руководитель подразделения, организационно-правовой отдел, а также назначенные для этого комиссии и должностные лица.

Примечание: Инструкция составляется для каждого конкретного защищаемого помещения с учетом его особенностей: назначения, проводимых конфиденциальных работ, хранимой и обрабатываемой информации, наличия технических средств, оборудования и т. д.

Продолжение приложения № 11

**Список работников, допущенных к вскрытию (закрытию)
защищаемого помещения № _____**

№ п/п	Фамилия, инициалы	Должность	Дополнительные полномочия	Примечание
1	2	3	4	5
1.				

Примечание: При лишении работника допуска в помещение (увольнение, перевод в другое подразделение и т.п.) в графе «Примечание» делается отметка о лишении допуска, например, «Уволен. Приказ от ____ № ____». Новый работник заносится в список. Записи заверяются подписью руководителя подразделения.

Перечень технических средств, установленных в помещении

№ п/п	Техническое средство	Тип	Учетный (инвентар- ный, заводской) номер	Дата уста- новки (удале- ния)	Класс техни- ческого средства (ОТСС или ВТСС)	Ответственный за эксплуатацию
1	2	3	4	5	6	7
1.						

Примечание:

ОТСС – основные технические средства и системы (в которых хранится и обрабатывается конфиденциальная информация).

ВТСС – вспомогательные технические средства и системы (которые размещаются вместе с ОТСС, но в которых не хранится и не обрабатывается конфиденциальная информация).

При удалении технического средства из помещения проставляется дата удаления в графе «Дата установки (удаления)».

Новые установленные технические средства вносятся в перечень.

**Список работников, ознакомленных с Техническим паспортом
на защищаемое помещение № ____**

№ п/п	Фамилия, инициалы	Подпись	Дата ознакомления	Примечание
1	2	3	4	5

Примечание. В список вносятся все работники, упомянутые в техническом паспорте.

