Приложение №2
к «Политике обработки персональных данных
СПб ГБУЗ «Городской противотуберкулезный диспансер»

ПОЛОЖЕНИЕ
об обработке и защите персональных данных пациентов в СПб ГБУЗ «Городской противотуберкулёзный диспансер»

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных пациентов СПб ГБУЗ «Городской противотуберкулезный диспансер" (далее по тексту - Положение) определяет порядок сбора, получения, учета, хранения, передачи, использования, уничтожения и любимых других видов обработки персональных данных пациентов СПб ГБУЗ «Городской противотуберкулезный диспансер» (далее по тексту – Оператор).

1.2. Положение разработано в соответствии с Конституции Российской Федерации, 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 от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в РФ», Постановлением Правительства РФ от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и другими действующими нормативными правовыми актами Российской Федерации (далее - Положение).

1.3. Целями настоящего Положения являются:

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

– защита персональных данных пациентов от несанкционированного доступа, разглашения, неправомерного их использования или утраты;

– определение порядка обработки персональных данных субъектов персональных данных пациентов.

1.4. Настоящее Положение и изменения к нему утверждаются главным врачом СПб ГБУЗ «Городской противотуберкулезный диспансер» и вводятся приказом.

1.5. Положение является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным пациентов.

1.6. Все работники Оператора, имеющие доступ к персональным данным пациентов должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

1.7. Настоящее Положение действует бессрочно, до замены его новым Положением.

2.Термины и определения

2.1. В настоящем Положении используются следующие основные понятия:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

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

Врачебная тайна - соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении.

Доступ к информации – возможность получения информации и ее использования.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным пациентов, требование не допускать их распространения без согласия пациента или иного законного основания.

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Пациенты (субъекты персональных данных) – физические лица (законные представители физических лиц), обратившиеся к Оператору с целью получения медицинского обслуживания, либо состоящие в иных гражданско-правовых отношениях с Оператором по вопросам получения медицинских услуг;

Персональные данные – персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено, или определяемо с помощью персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Понятие и состав персональных данных

3.1. Персональные данные пациента – информация, необходимая Оператору в связи с медицинским учетом и касающаяся конкретного пациента.

3.2. Перечень обрабатываемых Оператором персональных данных пациентов:

- фамилия, имя, отчество (при наличии);
- пол;

– дата (число, месяц, год) и место рождения;
– гражданство;
– паспортные данные (вид, серия, номер, наименование органа, выдавшего его, дата выдачи);
– адрес места жительства и регистрации;
– документ об опекунстве (для представителей субъектов персональных данных);
– контактный телефон и адрес электронной почты;
– реквизиты полиса ОМС (ДМС);
– страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
– данные о состоянии здоровья, заболеваниях, диагнозе, случаях обращения за медицинской помощью;
– данные о составе семьи;
– иные персональные данные, при определении объема и содержания которых Оператор руководствуется настоящим Положением и законодательством Российской Федерации.

3.3. Персональные данные пациентов относятся к специальной категории персональных данных, обработка таких персональных данных должна осуществляться лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

3.4. Персональные данные пациентов являются конфиденциальными сведениями. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законодательством РФ.

4. Цели обработки персональных данных

4.1. Персональные данные обрабатываются с целью обеспечения соблюдения законов и иных нормативных правовых актов, в том числе:
– установление медицинского диагноза;
– оказания медицинских услуг, в том числе идентификации пациентов;
– отражения информации в медицинской документации;
– учет услуг при оказании медицинских услуг;
– предоставления сведений страховым компаниям;
– предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг;
– организация обеспечения лекарственными средствами льготных категорий жителей Санкт-Петербурга при оказании амбулаторно-поликлинической помощи.

5. Принципы и условия обработки персональных данных

5.1. Обработка персональных данных Оператором производится на основании соблюдении принципов:
– обработка персональных данных осуществляется на законной и справедливой основе;
– обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
– соответствия объема и содержания обрабатываемых персональных данных, способов обработки персональных данных заявленным целям обработки.;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;

– Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен Федеральным законом от 27.07.2006 г. №152-ФЗ "О персональных данных", договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;

– уничтожение либо обезличивание персональных данных по достижении целей обработки персональных данных или в случае утраты необходимости их достижения, если иное не предусмотрено Федеральным законодательством.

5.2. В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке персональных данных пациента обязаны соблюдать следующие условия:

5.2.1. Обработка персональных данных пациента может осуществляться исключительно в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, оформления договорных отношений с пациентом при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну в соответствии с законодательством Российской Федерации.

5.2.2. Все персональные данные пациента следует получать у него самого или у его полномочного представителя. Если персональные данные пациента, возможно, получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

5.2.3. Оператор не имеет права получать и обрабатывать персональные данные пациента, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 г. №152-ФЗ "О персональных данных".

6. Согласие на обработку персональных данных пациента

6.1. Получение персональных данных Оператором осуществляется путем представления их самим пациентом на основании его письменного согласия, за исключением случаев, прямо предусмотренных действующим законодательством РФ. Обработка персональных данных пациентов без их согласия допускается при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.2. В случаях, предусмотренных Федеральным законодательством, обработка персональных данных осуществляется только с согласия пациента в письменной форме. Равнозначным содержащему собственноручную подпись пациента и работника согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом № 152-ФЗ электронной подписью.

6.3. Пациент 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 даётся в письменной форме согласно форме, указанной в Приложении №1 к настоящему Положению, и должно быть конкретным, предметным, информированным, сознательным и однозначным.

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

6.5. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

6.6. Согласие пациента на обработку его персональных данных должно храниться вместе с его иной медицинской документацией.

6.7. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. 152-ФЗ «О персональных данных», возлагается на Оператора.

6.8. Персональные данные могут быть получены Оператором от лица, не являющегося субъектом персональных данных, при условии предоставления Оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. 152-ФЗ «О персональных данных».

6.9. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. 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, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. 152-ФЗ «О персональных данных». Форма отзыва согласия на обработку персональных данных представлена в Приложении №2.

7. Обработка персональных данных пациентов

7.1. Обработка персональных данных пациентов включает в себя следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача, блокирование, удаление, уничтожение персональных данных.

7.2. Обработка персональных данных пациентов осуществляется:

– после получения письменного согласия субъекта персональных данных, составленного по утверждённой Оператором форме;

– после направления уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

7.3. При сборе персональных данных пациентов Оператор по требованию пациента (субъекта персональных данных) предоставляет информацию о:

– факте обработки персональных данных Оператором;
– правовых основаниях н целях обработки персональных данных;
– целях и применяемых способах обработки персональных данных;
– наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании положений законодательства;

– обрабатываемых персональных данных, относящихся к субъекту персональных данных, источнике их получения, если иной порядок представления таких данных не предусмотрен положениями законодательства;

– сроках обработки персональных данных, в том числе сроки их хранения;

– порядке осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. №152-ФЗ "О персональных данных".

7.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных пациента осуществляется путем:

7.3.1 Предоставления пациентом Оператору своих персональных данных в документированной форме. Предъявляемыми документами являются:

– полис ОМС или ДМС;

– паспорт или иной документ, удостоверяющий личность пациента или законного представителя;

– страховой номер индивидуального лицевого счета (СНИЛС).

7.3.2 Внесение сведений в учетные формы.

7.3.3 Формирование персональных данных в ходе оказания медицинских услуг.

7.3.4 Внесение персональных данных в информационные системы Оператора, используемые медицинскими работниками.

7.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от пациента или его представителя.

7.6. Обработка персональных данных пациентов осуществляется смешанным путем:

– неавтоматизированным способом без использования автоматизированных средств;

– автоматизированным способом обработки персональных данных.

7.7. Все меры конфиденциальности при сборе, записи, систематизации, накоплении и уточнении (обновлении, изменении) персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

7.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

7.9. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки.

7.10. Персональные данные пациентов хранятся и в электронном виде на серверах Оператора и в персональных компьютерах работников, подключенных к локальной сети. Доступ к электронным базам данных ограничен паролем

7.11. Информация персонального характера пациента хранится и обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

7.12. Не допускается использовать информацию о пациентах за пределами рабочего времени и (или) в целях, не связанных с осуществлением своих трудовых обязанностей, а также после прекращения трудовых отношений с СПБ ГБУЗ «Городской противотуберкулезный диспансер».

7.13. Согласно Письму Минздрава России от 07.12.2015 №13-2/1538 «О сроках хранения медицинской документации», медицинская карта пациента, получающего медицинскую помощь хранится 25 лет, после чего подлежит уничтожению.

7.14. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях.

7.15. Срок хранения персональных данных пациентов определяется целью обработки персональных данных. По истечению срока хранения или утраты цели обработки персональные данные подлежат уничтожению, обезличиванию или передаче в архив.

8. Передача персональных данных пациентов

8.1. Передача персональных данных включает в себя такие действия как распространение и предоставление персональных данных пациента. Под предоставлением в данном случае понимаются действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц, а под распространением — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

8.2. Оператор не распространяет персональные данные пациентов неопределенному кругу лиц.

8.3. Для включения в создаваемые сообщества/группы Оператором в социальных сетях и мессенджерах можно отправлять ссылку на группу или приглашение потенциальным участникам, но нельзя включать участников в сообщества без их согласия.

8.4. Участники сообщества/группы должны быть скрыты руководителем сообщества.

8.5. При передаче персональных данных пациента третьим лицам Оператор должен соблюдать следующие общие требования:

– не сообщать персональные данные пациента третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законодательством;

– не сообщать персональные данные пациента в коммерческих целях без его письменного согласия;

– разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных функций.

8.6. Персональные данные пациента могут быть предоставлены его родственникам или членам его семьи, иным представителям только с письменного разрешения самого пациента либо его законного представителя. Форма согласия о передачи персональных данных пациента представлена в Приложении №3.

8.7. Передача персональных данных от Оператора или его представителей третьей стороне может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных. Форма согласия о передачи персональных данных пациента представлена в Приложении №3.

8.8. Не допускается сообщение сведений о состоянии здоровья пациента, диагнозе его заболевания и других сведений о пациенте с использованием средств связи (телефон, факс, Интернет) без письменного согласия пациента.

8.9. Вместе с тем, Федеральный закон от 21.11.2011 г. №323-ФЗ «Об основах охраны здоровья граждан в РФ» и Федеральный закон от 27.07.2006 г. №152-ФЗ "О персональных данных" допускают разглашение сведений, составляющих врачебную тайну и персональные данные, с письменного согласия пациента или его законного представителя другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях (опубликование фото-, видео - материалов в социальный сетях, на сайте СПб ГБУЗ «Городской противотуберкулезный диспансер» и т.д.).

Предоставление сведений о факте обращения пациента за оказанием медицинской помощи, сведений о состоянии его здоровья и диагнозе, иных сведений, полученных при его медицинском обследовании и лечении (врачебная тайна), без согласия гражданина или его законного представителя допускается:

– в целях проведения медицинского обследования и лечения пациента, который в результате своего состояния не способен выразить свою волю, если медицинское

вмешательство необходимо по экстренным показаниям для устранения угрозы жизни человека и если его состояние не позволяет выразить свою волю или отсутствуют его законные представители;

– при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

– по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

– в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ», для информирования одного из его родителей или иного законного представителя;

– в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

– в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых предусмотрена военная и приравненная к ней служба;

– в целях расследования несчастного случая на производстве и профессионального заболевания;

– при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

– в целях осуществления учета и контроля в системе обязательного социального страхования;

– в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ».

9. Доступ к персональным данным пациента

9.1. Доступ к персональным данным пациентов должен быть ограничен и регламентирован для предотвращения утечки данных.

9.2. При хранении материальных носителей с персональными данными пациентов должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

9.3. Внутренний доступ (доступ внутри организации).

Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом Главного врача. Доступ Работникам к персональным данным предоставляется исключительно для цели исполнения ими своих трудовых функций

9.4. Внешний доступ.

Персональные данные пациента могут представляться в государственные и негосударственные функциональные структуры:

– правоохранительные органы;

– органы статистики;

– страховые медицинские организации;
– органы социального страхования;
– вышестоящие подразделения муниципальных органов управления;
– управление Росздравнадзора по Санкт-Петербургу и Ленинградской области;
– Комитет по здравоохранению Санкт-Петербурга;
– территориальный фонд ОМС Санкт-Петербурга;
– отделы опеки и попечительства;
– комиссии по делам несовершеннолетних и защите их прав;
– другие лечебно-профилактические учреждения.

10. Обязанности Оператора

10.1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

10.2. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федеральным законом от 27.07.2006 N 152-ФЗ.

10.3. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение Оператором согласия на обработку персональных данных являются обязательными, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

10.4. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных частью 4 ст. 18 Федерального закона от 27.07.2006 N 152-ФЗ , до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

– наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
– цель обработки персональных данных и ее правовое основание;
– перечень персональных данных;
– предполагаемые пользователи персональных данных;
– установленные настоящим Федеральным законом права субъекта персональных данных;
– источник получения персональных данных.

10.5. Оператор при обработке персональных данных обязан:

10.5.1. Принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных пациентов.

10.5.2. Издавать документы, определяющие политику оператора в отношении обработки и защиты персональных данных пациентов.

10.5.3. Осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному законодательству и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, локальным актам оператора.

10.5.4. Производить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона.

10.5.5. Ознакомлять работников, непосредственно осуществляющих обработку

персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, а также с Политикой в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

10.5.6. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

10.6. Обязанности Оператора и сроки реагирования при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных представлены в Правилах рассмотрения запросов субъектов персональных данных или их представителей, утвержденных Оператором.

10.7. Обязанности Оператора и сроки реагирования по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных представлены в Правилах рассмотрения запросов субъектов персональных данных или их представителей, утвержденных Оператором.

10.8. При получении письменного согласия пациента на обработку персональных данных, разрешенных для распространения Оператор обязан не позднее трех рабочих дней с момента получения указанного согласия опубликовать информацию об условиях обработки, о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных для распространения.

10.9. По факту обнаружения недостоверных персональных данных или неправомерных действий с ними Оператор обязан отреагировать на выявленное нарушение в соответствии со ст. 21 Федерального закона "О персональных данных" от 27.07.2006 №152-ФЗ, в том числе в случае невозможности устранить, уничтожить персональных данных, а также уведомить о своих действиях Работника или уполномоченный орган.

11. Права пациента (субъекта персональных данных)

11.1. В целях защиты персональных данных, хранящихся у Оператора, пациент имеет право:

11.1.1. на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального законодательства РФ;
- обрабатываемые персональные данные, относящиеся к соответствующему пациенту, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством РФ;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные федеральным законодательством РФ, за исключением случаев, предусмотренных ч. 8 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Вышеуказанные сведения должны быть предоставлены пациенту Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

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

11.1.3. требовать от Оператора уточнения своих персональных данных, их изменения, исключения, блокирования или уничтожения в случае, если персональные данные являются неверными, неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. При отказе Оператора исключить или исправить персональные данные пациента, пациент имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия.

11.1.4. требовать извещения Оператора всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

11.1.5. получать от Оператора сведения о его наименовании и месте нахождения, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона. Требование оформляется в письменном виде.

11.1.6. требовать прекратить в любое время передачу (распространение, предоставление, доступ) персональных данных, разрешенных для распространения.

11.1.7. обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Оператора при обработке и защите его персональных данных.

Все запросы при обращении пациента (субъекта персональных данных) к Оператору рассматриваются и обрабатываются согласно Правилам рассмотрения запросов субъекта персональных данных или их представителей, утвержденных Оператором.

12. Защита персональных данных пациента

12.1. Под защитой персональных данных пациента понимается комплекс мер (организационных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

12.2. Для защиты персональных данных пациентов Оператор принимает следующие меры:

– осуществляет разработку локальных нормативных актов и инструкций по обеспечению защиты персональных данных;

– обеспечивает разграничение доступа к персональным данным;

– организует работу персонала с информацией, содержащей персональные

данные, в том числе с материальными носителями такой информации;

– принимает необходимые технические меры, направленные на ограничение доступа посторонних лиц к персональным данным.

12.3. С целью защиты персональных данных пациентов приказом главного врача назначается:

– работник, Ответственный за организацию обработки и защиту персональных данных пациентов;

– перечень должностей, при замещении которых обрабатываются персональные данные пациентов;

– перечень персональных данных пациента, к которым имеют доступ работники, занимающие должности, предусматривающие обработку персональных данных;

– порядок доступа в помещения, в которых ведется обработка персональных данных;

– форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;

– порядок защиты персональных данных при их обработке в информационных системах персональных данных;

– порядок осуществления внутреннего контроля соответствия условиям обработки персональных данных;

– порядок уничтожения информации;

– иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области персональных данных.

12.4. К обработке персональных данных пациентов допускаются только медицинские работники, прошедшие определенную процедуру допуска, к которой относятся:

– ознакомление работника под личную подпись с настоящим Положением и локальными нормативными актами организации (положения, инструкции и т.д.), строго регламентирующими порядок и процедуру работы с персональными данными. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных пациента, с данными актами также производится ознакомление под личную подпись.;

– подписание сотрудником Обязательства о неразглашении персональных данных и соблюдении конфиденциальности при работе с ними. Форма Обязательства представлена в Приложении №4;

– получение сотрудником и использование в работе индивидуальных атрибутов доступа к информационным системам, содержащих в себе персональные данные.

В трудовые договоры лиц, принимаемых на работу, связанную с получением, обработкой, хранением, передачей и использованием персональных данных пациентов, включается условие об обеспечении конфиденциальности персональных данных.

12.5. Перечень работников Оператора, имеющих доступ к персональным данным пациентов, утверждается главным врачом.

12.6. Работники учреждения, имеющий доступ к персональным данным пациентов в связи с исполнением трудовых обязанностей, обязуются выполнять следующие требования:

– не использовать без разрешения обладателя или субъекта его персональные данные в целях, не связанных с осуществлением трудовой функции;

– хранить информацию, содержащую персональные данные пациента, исключающую доступ к ним третьих лиц;

– в отсутствие работника на его рабочем месте не должно быть в свободном доступе документов, содержащих персональные данные пациентов;

– при уходе в отпуск, во время служебной командировки и в иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные пациентов лицу, на которое приказом главного врача будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные пациентов, передаются другому работнику, имеющему доступ к персональным данным пациентов, по указанию главного врача;

– при увольнении работника, имеющего доступ к персональным данным пациентов, документы и иные носители, содержащие персональные данные пациентов, передаются другому работнику, имеющему доступ к персональным данным пациентов, по указанию главного врача;

– не разглашать информацию, содержащую персональные данные пациентов, а также не совершать иных деяний, влекущих уничтожение или утрату такой информации (материальных и электронных носителей);

– незамедлительно сообщать об утрате или несанкционированном уничтожении персональных данных пациента своему непосредственному руководителю или Ответственному за обработку и защиту персональных данных пациентов, а также об иных обстоятельствах, создающих угрозу сохранения конфиденциальности персональных данных (в том числе о попытках неправомерного доступа со стороны неуполномоченных лиц).

12.7. При прекращении трудовых отношений с Оператором работник обязан сдать все материальные носители персональных данных пациентов, а также ключи от помещений и шкафов, в которых они хранятся.

12.8. Защита доступа к электронным базам данных, содержащим персональные данные пациентов, обеспечивается:

– использованием лицензированных антивирусных программ, файрволов и VPN шлюзов, не допускающих несанкционированный вход в локальную сеть учреждения и обеспечивающих защищенные каналы связи;

– разграничением прав доступа средствами аутентификации;

– двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли информационной системы персональных данных и сообщаются индивидуально работникам, имеющим доступ к персональным данным пациентов.

12.9. Для обеспечения внешней защиты персональных данных пациентов работники обязаны соблюдать ряд мер:

– порядок приема, учета и контроля деятельности посетителей;

– установление пропускного режима учреждения;

– технические средства охраны;

– порядок охраны территории, зданий, помещений;

– требования к защите информации при интервьюировании и собеседованиях;

– запрет работникам, имеющим доступ к персональным данным пациентов и конфиденциальной информации, раскрывать посторонним лицам распределение функций, рабочие процессы, технологию составления, ведения и хранения документации, рабочих материалов.

12.10. Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

13. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных пациента

13.1. Должностные лица, получающие доступ к персональным данным пациентов, дополнительно несут персональную ответственность за обеспечение конфиденциальности, предоставленной им информации.

13.2. К способам нарушения режима конфиденциальности персональных данных пациентов относятся:

– разглашение персональных данных пациентов;

– неправомерное использование персональных данных пациентов (использование без согласия субъекта и (или) в целях, не связанных с оказанием медицинской помощи пациенту);

– утрата документов и иных материальных носителей персональных данных пациентов;

– неправомерное уничтожение документов, содержащих персональные данные пациентов;

– нарушение требования хранения документов, содержащих персональные данные пациентов;

– передача документов и сведений, содержащих персональные данные неуполномоченным лицам;

– другие нарушения требований законодательства и настоящего Положения.

13.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации

13.4. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

13.5. При возникновении инцидента, повлекшего нарушение конфиденциальности, целостности и доступности персональных данных по вине должностных лиц и если это

повлекло за собой какие-либо финансовые потери для организации, виновные должностные лица обязаны возместить причиненный ущерб.

13.6. Неправомерность деятельности обработки персональных данных может быть установлена в судебном порядке по требованию субъекта персональных данных.

Разработано:

Специалист по защите информации Е.Е. Моисеева

Согласовано:

Зам. главного врача по клинико-экспертной работе Д.В. Воронов

Начальник отдела информационных технологий А.С. Богданов

Юрисконсульт Т.Б. Григорьева