Утверждено Приказом
главного врача БУЗ ВО
Вологодский областной
кожно-венерологический
диспансер от
15 октября 2021 г. №528

ПОЛОЖЕНИЕ
об обработке и защите персональных данных пациентов в БУЗ ВО «Вологодский областной кожно-венерологический диспансер»

1. Общие положения

1.1. Настоящее Положение утверждено в целях обеспечения требований защиты прав и персональных данных пациентов в БУЗ ВО «Вологодский областной кожно-венерологический диспансер» (Организации) от несанкционированного доступа, неправомерного их использования или утраты при обработке.

1.2. Настоящее Положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», Постановления Правительства РФ №1119 от 01.11.2012г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ №687 от 15.09.2008г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Федерального закона от 27.07.2006г. №149-ФЗ «Об информационных технологиях и о защите информации», Федерального закона от 21.11.2011г. №323- ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

2. Понятие состав персональных данных

2.1. Персональные данные пациента – информация, необходимая поликлинике в связи с договорными отношениями и касающиеся конкретного пациента. Под информацией о пациентах понимаются сведения о фактах, событиях и обстоятельствах жизни пациента, позволяющие идентифицировать его личность.

2.2. В состав персональных данных пациента входят:

1.Фамилия, имя, отчество;

2.Дата рождения;

3.Реквизиты документа, удостоверяющего личность;

4. Адрес регистрации и фактического проживания

5. Реквизиты полиса медицинского страхования;

6. Сведения о наличии льгот;

7. Данные о состоянии здоровья;

8. ИНН;

9.Данные о детях;

10. Данные о семейном положении;

3. Согласие субъекта на обработку его персональных данных

3.1. Обработка специальных категорий персональных данных, таких как состояние здоровья, допускается только с согласия субъекта персональных данных. Согласие должно быть получено от субъекта персональных данных в письменном виде.

3.2. Согласие должно содержать следующую информацию:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

4. Обработка персональных данных

4.1. Под обработкой персональных данных пациента понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных пациента.

4.2. В целях обеспечения прав и свобод человека и гражданина Организация и его представители при обработке персональных данных пациента обязаны соблюдать следующие общие требования:

4.2.1. Обработка персональных данных пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия пациентам в предоставлении услуг, обеспечения личной безопасности пациентов, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4.2.2. При определении объема и содержания обрабатываемых персональных данных пациента Организация должна руководствоваться Конституцией Российской Федерации, и иными федеральными законами.

4.2.3. Получение персональных данных может осуществляться как путем представления их самим пациентом, так и путем получения их из иных источников.

4.2.4. Персональные данные следует получать у него самого. Если персональные данные пациента возможно получить только у третьей стороны, то клиент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Организация должна сообщить клиенту о целях, предполагаемых источниках и способах

получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение.

4.3. К обработке, передаче и хранению персональных данных пациента могут иметь доступ сотрудники:

- сотрудники кадровой и экономической службы;
- сотрудники компьютерных отделов;
- медицинский персонал.

4.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

4.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

4.5. Передача персональных данных пациента возможна только с согласия пациента или в случаях, прямо предусмотренных законодательством.

4.5.1. При передаче персональных данных пациента Организация должна соблюдать следующие 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 законом;
- не сообщать персональные данные пациента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные пациента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными пациентов в порядке, установленном федеральными законами;
- 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;
- передавать персональные данные пациента представителям пациентов в порядке, установленном и ограничивать эту информацию только теми персональными данными пациента, которые необходимы для выполнения указанными представителями их функций.

4.5.2. Передача персональных данных от субъекта или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

4.5.3. При передаче персональных данных пациента потребителям (в том числе и в коммерческих целях) за пределы Организации, не должно сообщать эти данные третьей стороне без письменного согласия пациента, за исключением случаев, когда это

необходимо в целях предупреждения угрозы жизни и здоровью пациента или в случаях, установленных федеральным законом.

4.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных пациента распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

4.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

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

5. Защита персональных данных

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

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

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Организации.

5.4. Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена поликлиникой за счет ее средств в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами Организации.

5.5.2. Для обеспечения внутренней защиты персональных данных пациентов необходимо соблюдать ряд мер:

- ограничение и регламентация состава персонала, функциональные обязанности которых требуют конфиденциальных знаний;

- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;

- знание требований нормативно – методических документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава персонала, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками Организации;

- воспитательная и разъяснительная работа с сотрудниками Организации по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- не допускается выдача амбулаторных медицинских карт на рабочие места врачей вне времени приема конкретного пациента. Амбулаторные медицинские карты могут выдаваться на рабочие места только врачу, ведущему прием конкретного пациента, сотруднику, ответственному за защиту персональных данных для копирования и в исключительных случаях, по письменному разрешению Главного врача, - руководителю структурного подразделения (например, при подготовке материалов для ответа на обращение или жалобу).

5.5.3. Защита персональных данных пациентов на электронных носителях.

Все папки, содержащие персональные данные пациента, должны быть защищены паролем, который сообщается по запросу лечащему врачу и лицу, ответственному за защиту персональных данных в Организации.

5.6. «Внешняя защита».

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Организации, посетители, клиенты других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

5.6.3. Для обеспечения внешней защиты персональных данных пациентов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;

- пропускной режим Организации;

- учет и порядок выдачи удостоверений;

- технические средства охраны, сигнализации;

- порядок охраны территории, зданий, помещений, транспортных средств;

- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных пациентов.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, Организация, пациенты и их представители могут вырабатывать совместные меры защиты персональных данных пациентов.

6. Права и обязанности пациента

6.1. Закрепление прав пациента, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. Пациенты и их представители должны быть ознакомлены с документами Организации, устанавливающими порядок обработки персональных данных пациентов, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся в Организации, клиент имеет право:

- требовать исключения или исправления неверных или неполных персональных данных.

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

- 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 и семейной тайны.

- своевременно сообщать ответственным сотрудникам Организации об изменении своих персональных данных.

6.4. Пациенты ставят Организация в известность об изменении фамилии, имени, отчества, даты рождения.

6.6. В целях защиты частной жизни, личной и семейной тайны пациенты не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность – одно из главных требований функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

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

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

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

7.5.2. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на пациентов.

7.5.3. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов государственной власти и Организации по сбору и использованию персональных данных может быть установлена в судебном порядке.