ПОЛОЖЕНИЕ

ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ГОРОДСКАЯ БОЛЬНИЦА № 1 Г. ЕМАНЖЕЛИНСК»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным пациентов ГБУЗ «Городская больница № 1 г. Еманжелинск», далее Учреждения. Под пациентом понимается человек, получающий медицинскую помощь, подвергающийся медицинскому наблюдению и/или лечению по поводу какого-либо заболевания, патологического состояния или иного нарушения здоровья и жизнедеятельности, а также пользующийся медицинскими услугами независимо от наличия у него заболевания.

Цель

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных пациентов, хранящихся в Учреждении, посредством планомерных действий по совершенствованию системы защиты персональных данных.

Основания

Основанием для разработки данного Положения являются:

- Конституция РФ от 12.12.1993;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных".
- Федеральный закон № 24 – ФЗ от 20.02.1995 «Об информации, информатизации и защите информации»;
- Указ Президента РФ № 188 от 06.09.1997 «Об утверждении перечня сведений конфиденциального характера».
- Постановление Правительства РФ от 17 ноября 2007 года № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".
- Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Порядок ввода в действие Положения о защите персональных данных и изменений к нему

Положение о защите персональных данных и изменения к нему вводятся приказом главного врача Учреждения. Все сотрудники Учреждения, допущенные к работе с персональными данными пациентов, должны быть ознакомлены с данным Положением и изменениями к нему, под распись.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Под персональными данными пациента понимается информация, необходимая Учреждению в связи с оказанием медицинской помощи и медицинских услуг и касающаяся конкретного пациента. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

– Фамилия, имя, отчество;
– пол
– дата рождения;
– адрес проживания;
– контактный телефон;
– реквизиты паспорта;
– данные полиса обязательного медицинского страхования или добровольного медицинского страхования;
– СНИЛС;
– инвалидность;
– данные о месте работы и профессии;
– данные о состоянии здоровья;
– данные о заболеваниях;
– данные лабораторных и параклинических исследований;
– данные о случаях обращения за медицинской помощью с любой целью.
– другие данные, относящиеся к персональным данным пациента, и дающие возможность идентифицировать его.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законом.

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который обратился за медицинской помощью в Учреждение. Субъект персональных данных самостоятельно решает вопрос передачи Учреждению своих персональных данных.

Держателем персональных данных является Учреждение, которому пациент добровольно передает во владение свои персональные данные. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

Получение, хранение, комбинирование, передача или любое другое использование персональных данных пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, для оказания медицинской помощи и медицинских услуг. Все персональные данные пациента получаются у него самого.

Материальными носителями персональных данных пациента являются медицинская карта амбулаторного больного, медицинская карта стационарного больного и документы медицинской статистики.

Медицинская карта амбулаторного больного заводится при первом обращении пациента в поликлинику и является собственностью учреждения. Медицинская карта стационарного больного заводится при каждой госпитализации пациента в стационарное отделение учреждения и также является собственностью учреждения.

Персональные данные, данные о состоянии здоровья и заболеваниях пациента, внесенные в медицинские карты и документы медицинской статистики, иные сведения, содержащиеся в медицинских картах и документах медицинской статистики, относятся к сведениям конфиденциального характера.

Медицинские карты амбулаторного пациента хранятся в регистратурах учреждения. Медицинские карты стационарного больного хранятся в оргметодкабинете. Все документы хранятся в металлических, закрывающихся на ключ, шкафах. Помещения, где хранятся медицинские карты амбулаторного пациента, и медицинские карты стационарного больного в конце рабочего дня закрываются на ключ и пломбируются. Доступ посторонних лиц в данные помещения строго запрещен

При обработке персональных данных пациентов Учреждение, в лице главного врача, вправе определять способы обработки, документирования, хранения и защиты персональных данных пациентов на базе современных информационных технологий.

Пациент имеет право на:

– полную информацию о своих персональных данных и обработке этих данных;
– свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные пациента, за исключением случаев, предусмотренных законодательством РФ;
– определение своих представителей для защиты своих персональных данных;
– доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;
– требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе Учреждения исключить или исправить персональные данные пациента, он имеет право заявить в письменной форме Учреждению о своем несогласии с соответствующим обоснованием такого несогласия.

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

Персональные данные добровольно передаются пациентом непосредственно держателю этих данных и потребителям внутри Учреждения, исключительно для обработки и использования в работе.

4.1.Внешний доступ. К числу массовых потребителей персональных данных вне Учреждения можно отнести государственные и негосударственные функциональные структуры:

– медицинские учреждения;
– органы Фонда обязательного медицинского страхования

- страховые медицинские организации;
- органы Фонда социального страхования;
- правоохранительные органы;
- военкоматы;

4.2.Внутренний доступ. Внутри Учреждения к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- главный врач и его заместители;
- заведующие отделениями;
- врачи;
- медсестры;
- медрегистраторы;
- медстатисты;
- фельдшеры ФАПов
- диспетчер по приему вызовов СМП;
- сотрудники отдела информатизации и информационной безопасности;

4.3. Порядок допуска к конфиденциальной информации.

4.1. Свободный доступ к персональным данным пациентов учреждения, закрывается с целью защиты их носителей. Лица, не имеющие доступа к персональным данным пациентов, применительно к ним относятся к категории посторонних.

4.2. Работник, который в силу своих служебных обязанностей имеет доступ к персональным данным, а также работник, которому будут доверены персональные данные для исполнения определенного задания, обязан в момент приема на работу либо по первому требованию главного врача Учреждения ознакомиться с настоящим Положением и подписать обязательство о неразглашении персональных данных пациентов учреждения.

4.3. Допуск к персональным данным осуществляется только после подписания работником обязательства о неразглашении персональных данных. Допуск осуществляется по решению главного врача, которое оформляется в виде приказа в письменной форме и доводится до сведения работника под роспись.

4.4. Обязательство о неразглашении персональных данных пациента оформляется в письменной форме за подписью работника и является неотъемлемой частью трудового договора, заключаемого с Учреждением.

4.5. Обязательство о неразглашении персональных данных пациентов оформляется в 3-х экземплярах, один из которых хранится в отделе кадров Учреждения (в личном деле работника), второй в отделе информатизации и информационной безопасности в месте с карточкой пользователя (доступа к конфиденциальной информации), а третий – передается работнику.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

При передаче персональных данных пациентов учреждение должно соблюдать следующие требования:

Передача внешнему потребителю:

– передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

– при передаче персональных данных пациента потребителям (в том числе и в коммерческих целях) за пределы Учреждения, эти данные, не должен сообщаться 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;

– ответы на правомерные письменные запросы других учреждений и организаций даются с разрешения главного врача Учреждения и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;

– не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;

– по возможности персональные данные обезличиваются.

Передача внутреннему потребителю. Учреждение вправе разрешать доступ к персональным данным пациентов. Потребители персональных данных должны подписать обязательство о неразглашении персональных данных пациентов (Приложение №1).

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

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.

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.

Защита персональных данных представляет собой жестко регламентированный 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 Учреждения.

6.1. «Внутренняя защита»

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

полномочий руководителями и специалистами Учреждения. Для защиты персональных данных пациентов необходимо соблюдать ряд мер:

– ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;

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

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

– знание сотрудниками 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 сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника и материальные носители;

– организация порядка уничтожения информации;

– своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;

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

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

6.2. «Внешняя защита»

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся 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.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения медицинских документов в учреждении.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

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

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

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.