Приложение № 1
к приказу № 125-Д от 18.11.2015 г.

УТВЕРЖДАЮ
Генеральный директор
ЛПУ «Родильный дом №2»
Г.Н.Суркова
«18» ноября 2015г.

ПОЛОЖЕНИЕ

ОБ ОРГАНИЗАЦИИ РАБОТЫ
С ПЕРСОНАЛЬНЫМИ ДАННЫМИ
ПАЦИЕНТОВ ЛПУ «РОДИЛЬНЫЙ ДОМ №2»

1. Общие положения

1.1. Целью данного Положения является защита персональных данных пациентов от несанкционированного доступа, неправомерного их использования или утраты.
1.2. Настоящее Положение разработано на основании Конституции РФ,
Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации», Федерального закона от 27 июля 2006 г. N **152**-**ФЗ** "О персональных данных" (с изменениями и дополнениями).
1.3. Персональные данные относятся к категории конфиденциальной информации.
Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 25 лет срока хранения, если иное не определено законом.
1.4. Настоящее Положение утверждается и вводится в действие приказом генерального директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным пациентов.

2. Понятие и состав персональных данных

2.1. Персональные данные пациента – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, другая информация, (ст. 3 ФЗ от 27 июля 2006 г. N 152-ФЗ "О персональных данных").
Пациент - любое физическое лицо, обратившееся за получением лечебно-диагностических (медицинских), диагностических, реабилитационных, медико-социальных и пр. аналогичных услуг в Лечебно–профилактическое учреждение «Родильный дом №2» (Далее Учреждение).
2.2. В состав персональных данных пациента могут входить:
- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- адрес места жительства;
- домашний телефон;
- биографические и биометрические данные, полученные от пациента при обращении в Учреждение и (или) ставшие известными Учреждению в процессе осуществления своей деятельности;
-данные о состоянии здоровья;
- копии отчетов, направляемые в органы статистики.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

3.1. 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.
3.2. В целях обеспечения прав и свобод человека и гражданина сотрудники Учреждения при обработке персональных данных работника обязаны соблюдать следующие общие требования:
3.2.1. Обработка персональных данных пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.
3.2.2. При определении объема и содержания обрабатываемых персональных данных пациента Учреждение должно руководствоваться Конституцией Российской Федерации, и иными федеральными законами.
3.2.3. Получение персональных данных может осуществляться путем представления их самим пациентом.
3.3. К обработке, передаче и хранению персональных данных пациента могут иметь доступ:
- сотрудник бухгалтерии;
- сотрудник информационно-технического отдела;
- сотрудники Учреждения, непосредственно работающие с пациентами или их персональными данными.
3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
3.4.1. 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.
3.5. Передача персональных данных пациента возможна только с согласия пациента или в случаях, прямо предусмотренных законодательством.
3.5.1. При передаче персональных данных пациента должны соблюдаться 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 пациентов, которые необходимы для выполнения конкретных функций;
- передавать персональные данные пациента представителям пациента в порядке, установленном законодательством, и ограничивать эту информацию только теми персональными данными пациента, которые необходимы для выполнения указанными представителями их функций.
3.5.2. 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.
3.5.3. При передаче персональных данных пациента потребителям (в том числе и в коммерческих целях) за пределы организации, Учреждение 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.
3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных пациента распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри Учреждения).
4.1.1. Право доступа к персональным данным пациента имеют:
- сам пациент, носитель данных.
- сотрудники Учреждения при выполнении ими своих служебных обязанностей.
4.1.2. Перечень лиц, имеющих доступ к персональным данным пациента, определяется приказом генерального директора.
4.2. Внешний доступ.
4.2.1. К числу массовых потребителей персональных данных вне Учреждения можно отнести государственные и негосударственные функциональные структуры:
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые компании;
- органы социального страхования;
- подразделения федеральных и муниципальных органов управления;
4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
4.2.3. Другие лица.
Персональные данные пациента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента.

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 компании.
5.4. Защита персональных данных пациента от неправомерного их использования или утраты обеспечивается Учреждением за счет его 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 обеспечении внутренней защиты персональных данных пациента соблюдается ряд мер:
- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником 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 работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками;
- проведение воспитательной и разъяснительной работы с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
5.5.3. Защита персональных данных пациента на электронных носителях. Все папки, содержащие персональные данные пациента, защищены паролем.
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 Учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.
5.6.3. Для обеспечения внешней защиты персональных данных пациента соблюдается 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.
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, сотрудники Учреждения, пациенты и их представители могут вырабатывать иные совместные меры защиты персональных данных пациентов.

6. Уничтожение персональных данных

6.1. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.
6.2. Уничтожение персональных данных пациента производится по письменному запросу пациента, либо его законного представителя, но не ранее чем по истечению срока договорных отношений пациента с Учреждением.
6.3. Уничтожение персональных данных на бумажных носителях производится сотрудниками, выполняющими обработку персональных данных, путем уничтожения носителя, с последующим составлением акта.
6.4. Уничтожение персональных данных в электронном виде осуществляется путём удаления информации со всех носителей и резервных копий без возможности дальнейшего восстановления, с последующим составлением акта.

7. Ответственность, связанная с персональными данными

7.1. Персональная ответственность – одно из главных требований к организации 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 Учреждения, получающий для работы конфиденциальный документ, несет ответственность за сохранность носителя и конфиденциальность информации.
7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, 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 работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.
7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных пациента, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.
7.5.3. В соответствии с Гражданским Кодексом РФ лица, незаконными методами получившие информацию, составляющую служебную или коммерческую тайну, обязаны возместить причиненные убытки.
7.5.4. 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, либо лишением свободы, в соответствии с УК РФ.
7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.