Положение о защите персональных данных работников и пациентов

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников и пациентов от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано в соответствии требованиями Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона Российской Федерации от 27.07 2006 года № 149-ФЗ "Об информации, информатизации и защите информации", Постановлением Правительства РФ от 17.11.2007 № 781 «Об утверждении положения об обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ.

1.3. Персональные данные относятся к категории конфиденциальной информации.

1.4. Настоящее Положение утверждается и вводится в действие приказом главного врача и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников и пациентов.

2. Понятие и состав персональных данных

2.1. Персональные данные — информация, с помощью которой можно идентифицировать человека: ФИО, место и год рождения, адрес прописки, паспортные данные и т.д.

2.2. В состав персональных данных работника входят:
- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;

- сведения о социальных льготах;
- наличие судимостей;
- адрес места жительства;
- домашний и сотовый телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- подпись сотрудника

2.3. В состав персональных данных пациента входят:
- ФИО пациента и законного представителя;
- паспортные данные;
- сведения о социальных льготах;

- диагноз
- адрес места жительства;
- место работы, службы;
- домашний и сотовый телефон;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дает согласие пациент;
- фотография пациента;
- подпись пациента.

3. Обработка персональных данных

3.1. Под обработкой персональных данных понимается: получение, хранение, комбинирование, передача или любое другое использование персональных данных

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных обязаны соблюдать следующие общие требования

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. Обработка персональных данных пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов для амбулаторного, стационарного и оперативного лечения, медицинских осмотров.

3.2.3 Персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение

. 3.2.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

3.3. 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 граждан возможна только с согласия граждан или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных граждан работодатель должен соблюдать следующие требования:

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

- не сообщать персональные данные граждан в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные граждан, 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 граждан, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными граждан в порядке, установленном федеральными законами
; разрешать доступ к персональным данным граждан только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные граждан, которые необходимы для выполнения конкретных 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.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных граждан 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

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 организации).

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом главного врача ООО «МЛ МИЦАР».

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды
- и др, согласно законодательства Российской Федерации

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.2.4. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.
В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (УК РФ)

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. 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 граждан от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральными законами.

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 работников необходимо соблюдать 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 подразделения;

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

5.5.3. Защита персональных данных граждан на электронных носителях. Все папки, содержащие персональные данные граждан, должны быть 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

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

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

6.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

6.2. 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.

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

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

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

6.5.1. 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.

6.5.2. Материальная ответственность работодателя и его представителей наступает в случае причинения лицу материального ущерба нарушением норм о защите его персональных прав.

6.5.3.Гражданско-правовая ответственность в связи с нарушением норм о защите персональных данных наступает в случае, когда лицу причинён имущественный и моральный ущерб.

6.5.4. В соответствии с Кодексом РФ об административных правонарушениях нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах, неправомерный отказ в предоставлении лицу информации, либо предоставление заведомо недостоверной информации влечёт предупреждение или наложение административного штрафа.

6.5.5. В соответствии с Уголовным кодексом РФ незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия признаётся преступлением и наказывается штрафом либо обязательными работами, либо исправительными работами, либо арестом, либо лишением свободы.