

Министерство здравоохранения Свердловской области
**ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
СВЕРДЛОВСКОЙ ОБЛАСТИ**
«ЦЕНТРАЛЬНАЯ ГОРОДСКАЯ БОЛЬНИЦА № 20 город Екатеринбург»

620010, г.Екатеринбург, ул.Дагестанская, 3

тел.: 258-96-68, факс: 258-94-69

№ 702

«31» декабря 2020 г.

ПРИКАЗ

**ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОБРАБОТКЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ**

Во исполнение Федеральных законов от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение о об обработке персональных данных пациентов Государственного автономного учреждения здравоохранения Свердловской области «Центральная городская больница № 20».
2. Заместителю главного врача по организационно-методической работе организовать размещение Положения на официальном сайте ГАУЗ СО «ЦГБ № 20», а также рассылку Положения в подразделения ГАУЗ СО «ЦГБ № 20».
3. Контроль исполнения приказа оставляю за собой.

Главный врач



С.М. Хмельникер

УТВЕРЖДАЮ

Главный врач
ГАУЗ СО «ЦГБ № 20»

С.М. Хмельникер

« 31 » 12 2020 г.

№ 701

ПОЛОЖЕНИЕ

**Об обработке и защите персональных данных пациентов
Государственного автономного учреждения здравоохранения
Свердловской области « Центральная городская больница № 20 город
Екатеринбург»**

Г. Екатеринбург
2021

1. Общие положения

Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.1997 №188, Федеральным законом от 29.07.2004 №98-ФЗ «О коммерческой тайне», с нормами Федерального закона от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» и другими нормативными актами, действующими на территории Российской Федерации.

Настоящее Положение определяет порядок обработки, сбора, хранения, передачи и любого другого использования персональных данных пациентов в ГАУЗ СО «ЦГБ №20» (далее – Оператор) и гарантии конфиденциальности сведений, предоставляемых пациентом.

2. Понятие и состав персональных данных пациентов

В настоящем Положении использованы следующие термины и определения:

Пациенты – граждане РФ, иностранные граждане, лица без гражданства.

Персональные данные пациента - паспортные данные (Ф.И.О., пол и дата рождения, адрес места жительства), данные о состоянии здоровья.

Обработка персональных данных - действия (операции) с персональными данными, включая получение, накопление, систематизацию, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

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.

Защита персональных данных работника – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном пациенте, полученной оператором в связи с лечением пациента.

Конфиденциальная информация – это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.

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

К персональным данным пациента относятся:

- Фамилия, имя, отчество, год, месяц, дата и место рождения, пол, адрес электронной почты, СНИЛС, гражданство, данные документа удостоверяющего личность, данные документа удостоверяющего личность за пределами Российской Федерации, данные документа, содержащиеся в свидетельстве о рождении, профессия, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- Данные о состоянии здоровья;
- Данные медицинского характера в случаях, предусмотренных законодательством;
- Данные о членах семьи пациента;
- Данные о месте жительства, адрес регистрации, почтовый адрес, телефон пациента, а также членов его семьи;
- Данные о социальных льготах (в том числе, об инвалидности), данные полиса ОМС (ДМС);
- Иные персональные данные, при определении объема и содержания которых оператор руководствуется настоящим Положением и законодательством Российской Федерации.

3. Сбор, обработка и защита персональных данных пациента

Персональные данные пациента относятся к конфиденциальной информации, то есть порядок работы с ними регламентирован действующим законодательством РФ и осуществляется соблюдением строго определенных правил и условий.

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

Сбор персональных данных пациента.

При поступлении в стационар или поликлинику пациент предоставляет персональные данные о себе в документированной форме. Предъявляемыми документами являются:

- полис ОМС или ДМС;
- паспорт или иной документ, удостоверяющий личность пациента или родителя;
- страховое свидетельство государственного пенсионного страхования;

После оформления пациента в регистратуре поликлиники или приемном отделении к документам, содержащим персональные данные пациента, также будут относиться:

- Медицинская карта стационарного больного;
- Амбулаторная карта.

Лица, получающие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными пациентов в порядке, установленном федеральными законами.

Защита персональных данных пациентов от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральными законами.

- **Обработка персональных данных пациентов** – это получение, хранение, комбинирование, передача или любое другое использование персональных данных пациентов.
- Обработка персональных данных пациентов может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в оказании медицинской помощи, контроля качества и объема оказанной медицинской помощи, пользования льготами, предусмотренными законодательством Российской Федерации;
- При определении объема и содержания, обрабатываемых персональных данных пациента оператор должен руководствоваться Конституцией РФ и иными федеральными законами;
- Все персональные данные пациента следует получать лично у пациента, его родителя или его законного представителя.

При обработке персональных данных пациента оператор должен соблюдать следующие требования:

Не сообщать персональные данные пациента в коммерческих целях без его личного письменного согласия, согласия родителя или законного представителя;

Предупреждать 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;

Разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, 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 настоящим Положением, и ограничивать эту информацию только теми персональными данными пациента, которые необходимы для выполнения указанными представителями их функций.

Получение персональных данных пациента.

Все персональные данные о пациенте оператор может получить у него самого, родителя или законного представителя.

Пациент обязан предоставить оператору полные и достоверные данные о себе, в случае изменения сведений, составляющих персональные данные пациента, незамедлительно предоставить данную информацию оператору. Оператор имеет право проверять достоверность сведений, предоставленных пациентом, сверяя данные, предоставленные пациентом, с имеющимися у пациента документами.

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. Оператор должен сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, данные о полисе обязательного медицинского страхования в страховой компании при отсутствии такового у пациента или при возникновении сомнений в правильности предоставляемых пациентом данных и т.п.) и последствиях отказа пациента дать письменное согласие на их получение;

Хранение персональных данных пациента.

Пациенты и их представители могут быть по желанию ознакомлены с документами организации, устанавливающими порядок обработки персональных данных пациентов, а также осведомлены об их правах в этой области.

Оператор должен вырабатывать меры защиты персональных данных пациентов.

Персональные данные пациентов на бумажных носителях хранятся у врачей отделений в период лечения, у врачей поликлиники в период обследования, в регистратуре поликлиники в течение 2-х лет после последнего обращения, в архиве оператора после окончания лечения в течение утвержденного законодательством срока. На электронных носителях персональные данные пациентов хранятся в отделе информационно-медицинского обеспечения (в виде электронной базы данных на рабочих серверах и в архивных файлах на серверах резервного копирования). Приемное отделение стационара и регистратура поликлиники имеют постоянный доступ к базам данных пациентов посредством рабочих станций локальной компьютерной сети, обеспеченной системой паролей. Все вышеописанные службы оператора обеспечивают защиту персональных данных пациентов от несанкционированного доступа и копирования.

Хранение персональных данных пациентов в иных структурных подразделениях оператора, сотрудники которых имеют право доступа к персональным данным, осуществляется в порядке, исключающем к ним доступ третьих лиц.

Конкретные обязанности по хранению персональных данных пациентов, заполнению и распечатке историй болезни и амбулаторных карт, формированию счетов в страховые компании возлагаются на работников конкретных подразделений оператора и закрепляются в должностных инструкциях.

В отношении некоторых документов действующим законодательством РФ могут быть установлены иные требования хранения, чем предусмотрено настоящим Положением. В таких случаях следует руководствоваться правилами, установленными соответствующим нормативным актом.

Сотрудник оператора, имеющий доступ к персональным данным пациентов в связи с исполнением трудовых обязанностей:

- Обеспечивает хранение информации, содержащей персональные данные пациентов, исключающее доступ к ним третьих лиц

В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные пациентов (соблюдение «политики чистых столов»), при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные носители, содержащие персональные данные пациентов, лицу, на которое распоряжением руководителя будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные пациентов, передаются другому сотруднику, имеющему доступ к персональным данным пациентов, по указанию руководителя.

При увольнении сотрудника, имеющего доступ к персональным данным пациентов, документы и иные носители, содержащие персональные данные пациентов, передаются другому сотруднику, имеющему доступ к персональным данным пациентов, по указанию руководителя.

В случае реорганизации или ликвидации организации оператора учет и сохранность документов, порядок передачи их на государственное хранение осуществлять в соответствии с правилами, предусмотренными учредительными документами.

Использование (доступ, передача, комбинирование) персональных данных пациента.

Оператор обеспечивает ограничение доступа к персональным данным пациентов лицам, не уполномоченным законом либо оператором для получения соответствующих сведений.

Доступ к персональным данным пациентов без специального разрешения имеют работники, занимающие следующие должности:

- Главный врач
- Заместители главного врача
- Заведующий отделением
- Старшая медицинская сестра
- Врач отделения
- Медицинская сестра отделения
- Экономист
- Медицинский регистратор
- Работники отдела информационно-медицинского обеспечения, непосредственно ведущие обработку информации для предоставления ее в страховые компании
- Работники архива
- Медицинские статистики

При получении сведений, составляющих персональные данные пациента, указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных функций, заданий.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией главного врача доступ к персональным данным пациента может быть предоставлен иному сотруднику, должность которого не включена в перечень

должностей сотрудников, имеющих доступ к персональным данным пациента, которому они необходимы в связи с исполнением трудовых обязанностей.

В случае если оператору оказывают услуги юридические и физические лица на основании заключенных договоров они должны иметь доступ к персональным данным пациентов, то соответствующие данные предоставляются оператором только после подписания с ними соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных пациентов.

Процедура оформления доступа к персональным данным пациента включает в себя:

- ознакомление работника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных пациента, с данными актами также производится под роспись.
- Истребование с сотрудника письменного обязательства о соблюдении конфиденциальности персональных данных пациента и соблюдении правил их обработки, подготовленного по установленной форме.

Передача персональных данных между подразделениями оператора осуществляется только между сотрудниками, имеющими доступ к персональным данным пациентов. При передаче персональных данных пациента оператор должен соблюдать следующие требования:

- Осуществлять защиту персональных данных пациента;
- Обеспечить хранение медицинской документации. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные;

Заполнение документации, содержащей персональные данные пациента осуществлять в соответствии с унифицированными формами медицинской документации.

Сотрудники оператора, передающие персональные данные пациентов третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные пациентов. Акт составляется по установленной форме и должен содержать следующие условия.

- уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;
- предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

Передача документов (иных материальных носителей), содержащих персональные данные пациентов, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг

- соглашения о неразглашении конфиденциальной информации; либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных пациента;
- договор или соглашение должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные пациента, ее перечень, цель использования, фамилия, имя, отчество и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных пациента несет работник, а также руководитель, осуществляющий передачу персональных данных пациента третьим лицам.

Предоставление персональных данных пациента государственным органам производится в соответствии с требованиями действующего законодательства и настоящим Положением.

Доступ к персональным данным пациента третьих лиц (физических и юридических)

Передача персональных данных пациента третьим лицам осуществляется только с письменного согласия пациента, которое оформляется по установленной форме и должно включать в себя:

- Фамилию, имя, отчество, адрес пациента, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе.
- Наименование и адрес оператора, получающего согласие пациента;
- Цель передачи персональных данных;
- Перечень персональных данных, на передачу которых дает согласие пациент;
- Срок, в течение которого действует согласие, а также порядок его отзыва.

Согласия пациента на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом.

Если лицо, обратившееся с запросом о персональных данных пациента не уполномочено федеральным законом на получение персональных данных пациента, оператор обязан отказать в предоставлении персональных данных лицу. Лицу обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных;

4. Организация защиты персональных данных пациента.

Защита персональных данных пациента от неправомерного их использования или утраты обеспечивается оператором.

Оператор обеспечивает:

- Ознакомление сотрудников под роспись с настоящим Положением.

При наличии иных нормативных актов (приказы, распоряжения, инструкции) регулирующих обработку и защиту персональных данных пациента, с данными актами также производится ознакомление сотрудников под роспись.

Истребование с сотрудников (за исключением лиц без специального разрешения) письменного обязательства о соблюдении конфиденциальности персональных данных пациента и соблюдении правил их обработки;

- Общий контроль за соблюдением сотрудниками оператора мер по защите персональных данных пациента.

Организацию и контроль за защитой персональных данных пациента в структурных подразделениях оператора, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

Защите подлежат:

- Информация о персональных данных пациента;
- Документы, содержащие персональные данные пациента;
- Персональные данные, содержащиеся на электронных носителях.

Защита сведений, хранящихся в электронных базах данных оператора, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

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

Иные права, обязанности, действия сотрудников, в трудовые обязанности которых входит обработка персональных данных пациентов, определяются также должностными инструкциями.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациентов, привлекаются к дисциплинарной, материальной, административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

Разглашение персональных данных пациентов (передача их посторонним лицам, в том числе работникам, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные пациентов, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями), влекут наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

Сотрудник оператора, имеющий доступ к персональным данным пациентов и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба пациенту или оператору.

Сотрудники оператора, имеющие доступ к персональным данным пациентов, виновные в незаконном разглашении или использовании персональных данных пациентов без согласия пациентов в корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со статьей 183 Уголовного кодекса Российской Федерации.

Неправомерный отказ оператора исключить или исправить персональные данные пациента, если отказ повлек за собой причинение вреда, а также любое иное нарушение прав пациента на защиту персональных данных влечет возникновение у пациента права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда.

6. Заключительные положения

Настоящее Положение вступает в силу с момента его утверждения главным врачом.

Настоящее Положение доводится до сведения всех работников персонально.

ГАУЗ СО «ЦГБ № 20» имеет право вносить изменения в настоящее ПОЛОЖЕНИЕ.

ГАУЗ СО «ЦГБ № 20» несет ответственность за нарушение обязательств по обеспечению безопасности и конфиденциальности персональных данных при их обработке в соответствии с законодательством Российской Федерации.