Утверждено
приказом по ОГБУЗ ОБ КО № 1
№674 «14» 09 2022 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных пациентов ОГБУЗ «Окружная больница Костромского округа № 1»

1. Общие положения

1.1. Положение об обработке и защите персональных данных пациентов (далее — «Положение») издано и применяется в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ» О персональных данных».

1.2. Настоящее Положение определяет порядок получения, обработки, учёта, накопления, хранения и защиты от несанкционированного доступа и разглашения сведений, составляющих персональные данные пациентов ОГБУЗ ОБ КО № 1 (далее «Учреждение»).

1.3. Обработка персональных данных пациентов организована Учреждением (оператором) на принципах законности, справедливости. Обработка проводится только персональных данных, которые отвечают целям их обработки, соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. Недопустимо объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. Хранение персональных данных проводится в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

1.4. Обработка персональных данных пациентов оператором осуществляется с соблюдением принципов и правил, предусмотренных Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и настоящим Положением.

1.5. Настоящее Положение и изменения к нему утверждаются главным врачом. При приеме на работу сотрудники знакомятся с настоящим Положением в отделе кадров под роспись. Положение размещено на официальном сайте больницы.

1.6. При обработке персональных данных оператор применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Роскомнадзора от 16.07.2010 № 482 «Об утверждении образца формы уведомления об обработке персональных данных» и иными документами.

2. Понятие, сбор и обработка персональных данных

2.1. Персональные данные пациентов – информация, необходимая Учреждению в связи с медицинским учетом и касающаяся конкретного пациента. К персональным данным пациента относятся:

- Фамилия, имя, отчество, год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности пациента;
- Данные о состоянии здоровья;
- Данные медицинского характера в случаях, предусмотренных законодательством;
- Данные о членах семьи пациента;

- Данные о месте жительства, работы, почтовый адрес, социальный статус, телефон пациента, а также членов его семьи;
- Иные персональные данные, при определении объема и содержания которых оператор руководствуется настоящим Положением и законодательством Российской Федерации.

2.2. 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 сотрудники при обработке персональных данных пациента обязаны соблюдать следующие общие требования:

2.3. 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 законного представителя;
- страховое свидетельство государственного пенсионного страхования (СНИЛС);

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

- медицинская карта стационарного больного;
- медицинская карта амбулаторного больного.

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.

2.4. 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.

Все персональные данные пациента следует получать лично у пациента 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 законного представителя;
- 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 его представителям, родственникам в случаях, установленных действующим законодательством РФ 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 или законного представителя. Согласие пациента на обработку его персональных данных должно храниться вместе с его медицинской документацией. Обработка персональных данных пациентов без их согласия допускается в соответствии с нормами действующего законодательства. Согласие на обработку персональных данных может быть отозвано пациентом. В случае отзыва пациентом согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия пациента при наличии оснований, указанных в действующем законодательстве (ч. 2 ст. 9 № 152-ФЗ).

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. 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.

В случае недееспособности пациента согласие на обработку его персональных данных дает его законный представитель.

Оператор не имеет право получать и обрабатывать персональные данные пациента о его политических, религиозных и иных убеждениях и частной жизни.

Хранение персональных данных пациента.

Пациенты и их представители могут по желанию ознакомиться с документами организации, устанавливающими порядок обработки персональных данных пациентов на официальном сайте больницы.

Персональные данные пациентов на бумажных носителях хранятся у врачей отделений в период лечения, у врачей поликлиник в период обследования, в регистратуре поликлиник, в архивах Учреждения в течение утвержденного законодательством срока, то есть до достижения цели обработки. На электронных носителях персональные данные пациентов хранятся в виде электронной базы данных на рабочих серверах и архивных файлах ОГБУЗ «МИАЦ», к которым у Учреждения есть доступ через ЗСПД.

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.

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 отсутствии сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные пациентов, при уходе в отпуск, 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.

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;
- секретарь (делопроизводитель);
- старшая медицинская сестра;
- главная медицинская сестра;
- младшая медицинская сестра по уходу за больными;
- заведующий отделением;
- медицинский статистик;
- юрисконсульт (главный, ведущий);
- сотрудник отдела медицинской статистики;
- сотрудник отдела автоматизированных систем управления;
- сотрудники отдела контроля качества оказания медицинской помощи;
- помощник врача-эпидемиолога;
- сотрудники планово-экономической службы;
- заместители главного врача по профилю;
- сотрудник бухгалтерии, планово-экономической службы;
- сотрудник регистратуры;
- врач, медицинская сестра, фельдшер.

2.14. Персональные данные вне Учреждения могут представляться в государственные и негосударственные функциональные структуры (внешний доступ) по запросам либо в рамках проводимых проверок:

- суды, органы прокуратуры, следствия, полиции;
- органы статистики, страховые медицинские организации, органы социального страхования;
- вышестоящие организации, проводящие проверки финансовой, медицинской деятельности Учреждения;
- территориальное управление Росздравнадзора по Костромской области;
- департамент здравоохранения по Костромской области;
- территориальный фонд ОМС по Костромской области;
- отделы опеки и попечительства;
- комиссии по делам несовершеннолетних и защите их прав;
- медицинские организации (при взаимодействии по оказанию медицинской помощи пациенту);
- органы власти и управления;
- в целях расследования несчастного случая на производстве и профессионального заболевания и др.

2.15. Персональные данные пациента могут быть предоставлены его законному представителю, родственникам, иным лицам в установленном законом случаях (ст. 13 № 323-ФЗ)

2.16. Оператор и иные лица, получившие доступ к персональным данным пациентов, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.17. Хранение персональных данных пациентов должно осуществляться в форме, позволяющей их идентифицировать.

2.18. Хранение персональных данных пациентов должно происходить в порядке, исключающим их утрату или их неправомерное использование.

2.19. Срок хранения персональных данных пациентов определяется действующим законодательством по хранению медицинской документации. По истечению срока хранения или утраты цели обработки персональные данные подлежат уничтожению, обезличиванию или передаче в архив.

2.20. Согласие пациента на передачу персональных данных не требуется, если законодательством РФ установлена обязанность предоставления оператором персональных данных (пп 2 - 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 № 152-ФЗ, ст. 13 № 323-ФЗ).

2.21. Трансграничная передача персональных данных пациентов в Учреждении не производится.

3. Права и обязанности оператора, пациентов в целях обеспечения защиты персональных данных пациентов

3.1. Оператор при обработке персональных данных обязан (ст. 21 № 152-ФЗ):

3.1.1. В случае выявления неправомерной обработки персональных данных при обращении пациента или его представителя либо по запросу пациента или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.1.2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.1.3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.2. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

3.3. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

3.4. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

3.5. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных п. 2 - 11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 № 152-ФЗ. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в ч. 3 - 5.1 ст. 21 № 152-ФЗ, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5. Ответственность

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациентов, привлекаются к ответственности в порядке, установленном действующим законодательством РФ.

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 доя работника ответственность, предусмотренную действующим законодательством РФ.

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.