

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ ИРКУТСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«ОБЛАСТНОЙ ОНКОЛОГИЧЕСКИЙ ДИСПАНСЕР»
(ГБУЗ ООД)



Утверждено

приказом главного врача

№ 18

03

2016 г.

№ 58

ПОЛОЖЕНИЕ

об обработке и защите персональных данных пациентов
в Государственном бюджетном учреждении здравоохранения
«Областной онкологический диспансер»

I. Общие положения

1.1. Настоящее Положение определяет порядок получения, обработки, хранения, передачи и любого другого использования персональных данных пациентов Государственного бюджетного учреждения здравоохранения «Областной онкологический диспансер» (далее по тексту — Учреждение).

1.2. Целями разработки настоящего Положения являются обеспечение Учреждением в соответствии с законодательством Российской Федерации обработки, хранения персональных данных пациентов, а также обеспечение защиты персональных данных от несанкционированного доступа, утраты, неправомерного их использования или распространения как на территории Учреждения, так и на Интернет-ресурсе Учреждения (официальном сайте).

1.3. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.2004 г. №98-ФЗ «О коммерческой тайне», Федеральным законом РФ от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», постановлением правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

1.4. В настоящем Положении используются следующие термины и

определения:

- Оператор персональных данных (далее по тексту — Оператор) — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. В настоящем положении под оператором подразумевается Учреждение.
- Субъект персональных данных (далее по тексту — Субъект) — физическое лицо предоставившее оператору свои персональные данные (пациент).
- Персональные данные (далее по тексту — ПД) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации в области здравоохранения, Положением об обработке и защите персональных данных и приказами Учреждения.
- Обработка персональных данных — действия (операции) с персональными данными, включая систематизацию, накопление, хранение, комбинирование, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
- Защита персональных данных — деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и обеспечение организационно-технических мер защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения.
- Конфиденциальная информация — это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.
- 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.

II. Сбор и обработка персональных данных субъектов персональных данных

2.1. Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Сбор и обработка персональных данных пациентов осуществляется исключительно с письменного согласия субъекта. Образцы форм согласий субъектов ПД на обработку персональных данных и отказа от нее, находятся в регистратуре, заполняются в первую очередь и вклеиваются в медицинскую карту пациента.

На Интернет-ресурсе Учреждения (официальном сайте) также размещаются формы согласия субъекта ПД на обработку персональных данных и отказа от нее и обязательно заполняются субъектами ПД в первую очередь, после чего субъекты ПД получают возможность оформить запрос в Учреждение о прохождении обследования и лечения. Персональные данные субъекта ПД относятся к конфиденциальной информации.

2.2. В целях обеспечения прав и свобод человека и гражданина оператор и его представители при обработке персональных данных субъекта ПД обязаны соблюдать следующие общие требования:

2.2.1. Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности, количества и качества выполняемой работы, обследования, наблюдения и лечения пациентов и обеспечения сохранности имущества оператора, пациента и третьих лиц.

2.2.2. Обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

2.2.3. Информация о персональных данных субъекта предоставляется оператору субъектом устно, путем заполнения медицинских карт для пациентов и журналов регистрации персональных данных, которые хранятся в регистратуре, архиве. Также информация о персональных данных субъекта может предоставляться оператору в информационно-телекоммуникационных сетях и иных информационных системах (Интернет-ресурс Учреждения (официальный сайт)).

2.2.4. Если персональные данные субъекта возможно получить только у третьей стороны, то сам субъект должен быть уведомлен об этом и от него

должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

2.2.4. Оператор не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и частной жизни.

2.2.5. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.3. При обращении в Учреждение пациент представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;
 - ИНН
 - полис ОМС;
 - в отдельных случаях с учетом специфики обследования в учреждение здравоохранения действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.
- Передача персональных данных пациентов вне учреждения разрешается только в установленных законом случаях.

III. Хранение и защита персональных данных субъектов персональных данных

3.1. Персональные данные субъектов хранятся на бумажных носителях в помещении регистратуры. Для этого используются специально оборудованные шкафы и сейфы. Медицинские карты прошедших обследование, лечение субъектов хранятся в архиве Учреждения. Также персональные данные могут храниться на электронных носителях.

3.2. Конкретные обязанности по ведению, заполнению медицинских карт субъектов, иных документов, отражающих персональные данные пациентов, возлагаются на работников регистратуры, администраторов и лечащих врачей.

3.3. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

3.4. При получении сведений, составляющих персональные данные субъектов заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных

функций и заданий.

3.5. Защита информации о персональных данных.

3.5.1. Сотрудники Учреждения, имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным.

3.5.2. Начальник отделения для обеспечения эксплуатации информационного оборудования Учреждения обеспечивает следующие меры по защите хранящейся на сервере информации:

- ограничение сетевого доступа на сервер для определенных пользователей;
- организация контроля технического состояния серверов и уровней защиты и восстановления информации;
- проведение регулярного резервного копирования информации;
- ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации.

3.5.3. Сотрудники Учреждения, имеющие доступ к персональным данным, при пользовании доступом в сеть Интернет обязаны принимать максимальные меры по обеспечению безопасности:

- установить и использовать антивирусное ПО (с обновлением баз вирусов);
- установить и использовать брандмауэр;
- устанавливать обновление для операционной системы.

3.5.4. Защита персональных данных пациентов в Учреждении возлагается на начальника отделения для обеспечения эксплуатации информационного оборудования.

IV. Передача персональных данных субъектов ПД

4.1. При передаче персональных данных субъектов сотрудники Учреждения, имеющие доступ к персональным данным, должны соблюдать следующие требования:

4.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных федеральными законами.

4.1.2. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению оператора, отсутствует угроза жизни или здоровью субъекта, оператор обязан отказать в предоставлении персональных данных лицу.

4.1.3. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

4.1.4. Предупредить лиц, получающих персональные данные субъекта, 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.

4.1.5. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

V. Обязанности субъекта и оператора ПД

5.1. В целях обеспечения достоверности персональных данных субъект обязан:

5.1.1. Предоставить оператору полные достоверные данные о себе.

5.2. Оператор обязан:

5.2.1. Осуществлять защиту персональных данных субъектов.

5.2.2. Обеспечить хранение учетной и 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.

5.2.3. Субъекты или их законные представители должны быть ознакомлены с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

5.2.4. Все сотрудники, имеющие доступ к персональным данным пациентов, обязаны подписать соглашение о неразглашении персональных данных.

VI. Права субъектов в целях защиты персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся у оператора, субъекты имеют право на:

6.1.1. Полную и безвозмездную информацию об их персональных данных и обработке этих данных.

6.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом.

6.1.3. Определение своих представителей для защиты своих персональных данных.

6.1.4. Требование об извещении оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.5. Обжалование в суд любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

VII. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к ответственности в порядке, установленном Кодексом РФ об административных правонарушениях и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

VIII. Заключительные положения

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

8.2. Настоящее Положение находится в свободном доступе как на территории Учреждения, так и на Интернет-ресурсе Учреждения (официальном сайте) доводится для ознакомления с ним всех субъектов ПД.

СОГЛАСОВАНО:

Главный врач



В.В. Дворниченко

Начальник отделения
для обеспечения эксплуатации
информационного оборудования



В.Н. Уцын

Начальник юридического отдела

О.Ю. Пархоменко