



«УТВЕРЖДАЮ»
Директор
ГБУЗ «СЛБ КНПЦСМП(о)»
В.М. Моисеенко
«15» октябрь 2013г.

Положение
об обработке персональных данных
в государственном бюджетном учреждении здравоохранения «Санкт-Петербургский
клинический научно - практический центр специализированных видов медицинской
помощи (онкологический)»

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных в государственном бюджетном учреждении здравоохранения «Санкт-Петербургский клинический научно - практический центр специализированных видов медицинской помощи (онкологический)» (далее – Положение) принято в целях обеспечения требований защиты прав граждан при обработке персональных данных.

1.2. Настоящее Положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положений статей 85-90 Трудового кодекса Российской Федерации.

1.3. В настоящем Положении используются следующие понятия и термины:

- Учреждение – государственное бюджетное учреждение здравоохранения «Санкт-Петербургский клинический научно - практический центр специализированных видов медицинской помощи (онкологический)»;
- субъекты персональных данных – пациенты Учреждения;
- персональные данные – информация, необходимая Учреждению для оказания услуг специализированной медицинской помощи и касающаяся конкретных пациентов и работников.
- служебные сведения (служебная тайна) – информация (сведения), доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.
- обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

1.4. Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью учреждения, в частности для оказания услуг специализированной медицинской помощи и делопроизводства. Учреждение собирает данные только в объеме, необходимом для достижения названных целей.

1.5. Сбор, хранение, использование персональных данных без согласия работников и пациентов, или их законных представителей, чьи данные вносятся в базы, не допускаются.

1.6. Распространение данных, в том числе передача третьим лицам, без письменного согласия, не допускается.

1.7. Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

1.8. Сотрудники Учреждения, в обязанность которых входит обработка персональных данных пациентов, обязаны обеспечить каждому пациенту, или их законному представителю, возможность ознакомления с документами и материалами, непосредственно затрагивающими права и свободы пациентов, если иное не предусмотрено законом.

2. Классификация и состав персональных данных

2.1. Учреждение обрабатывает персональные данные двух видов:

2.1.1. Персональные данные пациентов, получающих ОМС-услуги в соответствии с уставной деятельностью Учреждения. В состав персональных данных пациентов входят:

- фамилия, имя, отчество
- дата рождения
- место рождения
- паспортные данные
- семейное положение
- профессия
- адрес
- социальное положение
- образование
- национальная принадлежность
- состояние здоровья
- биометрические персональные данные

2.1.2. Персональные данные сотрудников. В состав персональных данных сотрудников входят:

- паспортные данные;
- образование;
- сведения о стаже работы по специальности (профессиональной категории);
- контактные телефоны.

2.2. Материалы личных дел пациентов относятся к конфиденциальной информации ограниченного доступа – класс 1 (К1).

2.3. Персональные данные сотрудников относятся к категории общедоступных – класс 4 (К4).

3. Принципы обработки персональных данных

Обработка персональных данных должна осуществляться на основе принципов:

- 3.1. Законности целей и способов обработки персональных данных и добросовестности;
- 3.2. Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;
- 3.3. Соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 3.4. Достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- 3.5. Уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- 3.6. Личной ответственности сотрудников Учреждения за сохранность и конфиденциальность персональных данных, а также носителей этой информации;
- 3.7. Наличие четкой разрешительной системы доступа сотрудников Учреждения к документам и базам данных, содержащим персональные данные.

4. Обязанности Учреждения

В целях обеспечения прав и свобод человека и гражданина Учреждение при обработке персональных данных обязано соблюдать следующие общие требования:

- 4.1. Осуществлять обработку персональных данных исключительно в уставных целях;

- 4.2. Хранить и защищать персональные данные от неправомерного их использования или утраты за счет его средств в порядке, установленном законодательством;
- 4.3. Блокировать персональные данные в случае выявления недостоверных персональных данных или неправомерных действий с ними;
- 4.4. Прекращать обработку персональных данных и уничтожить их в срок, не превышающий тридцати рабочих дней, в случае отзыва субъектом персональных данных согласия на их обработку;
- 4.5. Знакомить субъектов персональных данных под расписку с документами Учреждения, устанавливающими порядок обработки персональных данных пациентов, а также об их правах и обязанностях;
- 4.6. Передавать персональные данные в образовательные учреждения только с письменного согласия субъектов персональных данных.

5. Права субъектов персональных данных

- 5.1. Право на доступ к информации о самом себе.
- 5.2. Право на определение форм и способов обработки персональных данных.
- 5.3. Право на отзыв согласия на обработку персональных данных.
- 5.4. Право ограничивать способы и формы обработки персональных данных, запрет на распространение персональных данных без согласия.
- 5.5. Право требовать изменения, уточнения, уничтожения информации о самом себе.
- 5.6. Право обжаловать неправомерные действия или бездействия по обработке персональных данных.
- 5.7. Право на дополнение персональных данных оценочного характера путем подачи заявления с изложением собственной точки зрения.
- 5.8. Право определять представителей для защиты своих персональных данных.
- 5.9. Право требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них изменениях или исключениях из них.

6. Сбор, обработка и хранение персональных данных

- 6.1. Порядок сбора персональных данных пациентов:
 - 6.1.1. Персональные данные пациентов Учреждение получает от пациентов лично, от органов здравоохранения и у родственников. Органы здравоохранения уведомляют пациентов о передаче данных в Учреждение и получают письменное согласие. Письменное согласие прикладывается к пакету документов, содержащих персональные данные.
 - 6.1.2. Учреждение разрабатывает и утверждает формы предоставления персональных данных пациентов и получает персональные данные только в соответствии с этими формами.
 - 6.1.3. Информация о целях, предполагаемых источниках и способах получения персональных данных, формах их подачи, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение, размещается на сайте Учреждения и доводится не реже, чем один раз в год.
 - 6.1.4. В случае выявления недостоверных персональных данных или неправомерных действий с ними Учреждения при обращении или по запросу пациентов либо уполномоченного органа по защите прав субъектов персональных данных осуществляется блокирование персональных данных на период проверки.
 - 6.1.5. В случае подтверждения факта недостоверности персональных данных Учреждение на основании документов, представленных пациентом или их законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.
 - 6.1.6. В случае отзыва пациентом согласия на обработку персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить их в срок,

не превышающий тридцати дней с даты поступления указанного отзыва. Об уничтожении персональных данных Учреждение обязано письменно уведомить пациента.

6.1.7. Пациенты или их законные представители должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

6.1.8. Предоставление пациентам или их законным представителям доступа к персональным данным осуществляется только при наличии надлежащим образом оформленного запроса.

6.1.9. Доступ сотрудников Учреждения к персональным данным пациентов определён в разделе 7 настоящего Положения.

6.2. Порядок обработки персональных данных пациентов:

6.2.1. Обработка персональных данных осуществляется в целях определения состояния здоровья пациентов, обеспечивающих его право на доступное качественное медицинское лечение.

6.2.2. К обработке персональных данных пациентов могут иметь доступ медицинские работники Учреждения и сотрудники, имеющие определенный уровень доступа, участвующие в обработке персональных данных.

6.2.3. Процесс обработки персональных данных осуществляется коллегиально (комиссия, консилиум).

6.2.4. Результат обработки персональных данных оформляется в виде заключения.

6.2.5. Обработка персональных данных для статистических или иных научных целей осуществляется при условии обязательного обезличивания персональных данных.

6.2.6. Доверенные лица, получающие персональные данные пациентов, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Доверенные лица обязаны соблюдать режим конфиденциальности. Данное положение не распространяется в случае обезличивания персональных данных и в отношении общедоступных данных.

6.2.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

6.2.8. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

6.3. Хранение персональных данных.

6.3.1. Персональные данные пациентов хранятся в личных делах на бумажных и/или электронных носителях информации.

6.3.2. Персональные данные пациентов также могут храниться в базах данных локальной компьютерной сети учреждения. Доступ к электронным базам данных, содержащим персональные данные пациентов, обеспечивается парольной защитой.

6.3.3. Пароли выдаются системным администратором/специалистом по защите информации и меняются автоматически не реже чем 1 раз в 30 дней.

6.3.4. На рабочем столе сотрудника должен всегда находиться только тот массив документов и учетных карточек, с которым в настоящий момент он работает. Исполняемые документы не разрешается хранить россыпью. Их следует помешать в папки, на которых указывается вид производимых с ними действий (подшивка в личные дела, для отправки и пр.).

6.3.5. В конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы должны быть убраны с рабочего места сотрудника в стеллаж или тумбочку.

6.3.6. Учреждение особым образом обеспечивает гарантии конфиденциальности материалов, связанных с консультативной и диагностической деятельностью.

6.4. Порядок сбора, обработки и хранение персональных данных в отношении персональных данных сотрудников.

6.4.1. Сбор, обработка и хранение персональных данных осуществляется в целях исполнения договоров.

6.4.2. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе следующую информацию:

- подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки;
- способы обработки персональных данных, применяемые Учреждением;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

7. Доступ к персональным данным

7.1. Внутренний доступ (доступ внутри организации).

7.1.1. Право доступа к персональным данным пациентов имеют:

- директор Учреждения и заместители директора;
- заведующие отделений;
- лечащие врачи;
- старшие медсестры;
- медсестры;
- лаборанты;
- медрегистраторы;
- специалисты по безопасности персональных данных;
- системные администраторы.

7.2. Право на доступ к персональным данным сотрудников имеют:

- директор;
- администратор БД;
- бухгалтерия;
- отдел кадров.

7.3. Внешний доступ (доступ за пределами организации).

7.3.1. Право доступа к персональным данным пациентов.

- персональные данные пациентов могут быть предоставлены третьим лицам только с письменного согласия пациентов или их законных представителей;
- Учреждение обеспечивает ведение журнала учета выданных персональных данных пациентов, в котором фиксируются сведения о лице, которому передавались персональные данные пациента, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана;
- доступ третьих лиц к персональным данным пациентов предоставляется при получении запроса от них; запрос должен содержать информацию об организации, запрашивающей персональные данные, сведения о лице, ответственном за сохранение конфиденциальности, обоснование необходимости получения данных и письменное согласие пациентов или их законных представителей на передачу данных.

7.3.2. Право доступа к персональным данным сотрудников.

- Доступ третьих лиц к персональным данным сотрудников предоставляется при получении запроса от них; запрос должен содержать информацию об организации, запрашивающей персональные данные, включающую информацию об отношениях, связывающую её с данным субъектом персональных данных; сведения о лице,

ответственном за сохранение конфиденциальности; обоснование необходимости получения данных.

- Персональные данные сотрудников могут быть предоставлены третьим лицам при условии, что третье лицо представляет собой организацию, связанную трудовыми отношениями с субъектом персональных данных или отношениями административного руководства с работодателем сотрудника.

- Учреждение обеспечивает ведение журнала учета выданных персональных данных сотрудников, в котором фиксируются сведения об организации, которой передавались персональные данные сотрудника, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

8. Защита персональных данных

Для защиты персональных данных субъектов персональных данных соблюдается ряд мер:

8.1. Определён порядок приема, учета и контроля материалов, содержащих персональные данные.

8.2. Внедрены технические средства охраны, сигнализация.

8.3. Утверждены требования к защите информации.

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

8.5. Все лица, связанные с получением, обработкой и защитой персональных данных обязаны заключить «Обязательство о неразглашении персональных данных».

9. Уточнение, блокирование и уничтожение персональных данных

9.1. Блокирование информации, содержащие персональные данные, производится в случаях:

- если персональные данные являются неполными, устаревшими, недостоверными;
- если сведения являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

9.2. В случае подтверждения факта недостоверности персональных данных Учреждение на основании документов, представленных субъектом персональных данных, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязано уточнить персональные данные и снять их блокирование.

9.3. В случае выявления неправомерных действий с персональными данными Учреждение обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Учреждение в срок, не превышающий тридцати рабочих дней с даты выявления неправомерности действий с персональными данными, обязано уничтожить персональные данные.

9.4. Об устраниении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

9.5. Учреждение обязано уничтожить персональные данные в случае:

- достижения цели обработки персональных данных;
- отзыва субъектом персональных данных согласия на обработку персональных данных.

9.6. Уничтожение персональных данных должно быть осуществлено в течение тридцати рабочих дней от начала указанных выше моментов.

9.7. Учреждение должно направить уведомление об уничтожении персональных данных субъекту персональных данных, а в случае, если обращение или запрос о недостоверности персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанному органу.

10. Ответственность за разглашение персональных данных и нарушения.

10.1. Учреждение ответственно за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдение установленных в организации принципов уважения приватности.

10.2. Учреждение обязуется поддерживать систему приема, регистрации и контроля рассмотрения жалоб субъектов персональных данных, доступную как посредством использования Интернета, так и с помощью телефонной, телеграфной или почтовой связи.

10.3. Любое лицо может обратиться к директору Учреждения с жалобой на нарушение данного Положения. Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются директором в десятидневный срок со дня поступления.

10.4. Директор обязан на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб пациентов, а также содействовать исполнению требований компетентных органов. Сотрудники, виновные в нарушении требований настоящего положения, привлекаются к дисциплинарной ответственности.