

УТВЕРЖДАЮ

Главный врач

ФГБУ «ФЦН» Минздрава России
(г. Новосибирск)

_____ Д.А. Рзаев
«27» августа 2015 г.

ПОЛОЖЕНИЕ

об обработке персональных данных в информационных системах персональных данных федерального государственного бюджетного учреждения «Федеральный центр нейрохирургии» Министерства здравоохранения Российской Федерации
(г. Новосибирск)

На 9 листах

Новосибирск - 2015 г.

Содержание

1	Общие положения	3
2	Получение, обработка и защита персональных данных	4
3	Хранение персональных данных	5
4	Передача персональных данных	5
5	Уничтожение персональных данных	5
6	Внутренние проверки состояния защищенности информационной системы персональных данных	6
7	Обязанности субъекта персональных данных и Оператора	7
8	Права субъекта ПДн в целях защиты персональных данных	7
9	Реагирование на запросы субъектов ПДн и их законных представителей	8
10	Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн	8

1 Общие положения

1.1 Настоящее Положение об обработке персональных данных (далее – Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и любого другого использования персональных данных, обрабатываемых в информационной системе персональных данных (далее – ИСПДн) федерального государственного бюджетного учреждения «Федеральный центр нейрохирургии» Министерства здравоохранения Российской Федерации (г. Новосибирск) (далее – ФГБУ «ФЦН» Минздрава России (г. Новосибирск) или Оператор) в соответствии с законодательством Российской Федерации.

1.2 Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3 Для целей настоящего Положения используются следующие основные понятия:

- персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, 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 с персональными данными, совершаемые работниками ФГБУ «ФЦН» Минздрава России (г. Новосибирск) 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;

- автоматизированная обработка – обработка данных, выполняемая средствами вычислительной техники;

- 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;

- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных – система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

– защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном субъекте персональных данных.

1.4 Персональные данные, обрабатываемые в ФГБУ «ФЦН» Минздрава России (г. Новосибирск), относятся к конфиденциальной информации, порядок работы с которыми регламентирован Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и осуществляется с соблюдением строго определенных правил и условий.

2 Получение, обработка и защита персональных данных

2.1 Порядок получения персональных данных.

2.1.1 Все персональные данные следует получать лично у субъекта ПДн. Если персональные данные возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. ФГБУ «ФЦН» Минздрава России (г. Новосибирск) должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение.

2.1.2 ФГБУ «ФЦН» Минздрава России (г. Новосибирск) вправе обрабатывать персональные данные субъектов ПДн только с их письменного разрешения.

2.1.3 Письменное согласие субъекта ПДн на обработку своих персональных данных должно включать в себя персональные данные, указанные в перечне ПДн, подлежащих защите в ИСПДн ФГБУ «ФЦН» Минздрава России (г. Новосибирск) (Приложение № 1 к Положению).

2.1.4 Работники ФГБУ «ФЦН» Минздрава России (г. Новосибирск) области имеют право получать только те ПДн, которые необходимы им для выполнения своих служебных обязанностей.

2.1.5 Работники ФГБУ «ФЦН» Минздрава России (г. Новосибирск), получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности.

2.2 Порядок обработки персональных данных.

2.2.1 При определении объема и содержания, обрабатываемых персональных данных, ФГБУ «ФЦН» Минздрава России (г. Новосибирск) должен руководствоваться Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и иными федеральными законами в области защиты персональных данных.

2.2.2 При принятии решений, затрагивающих интересы субъекта ПДн, ФГБУ «ФЦН» Минздрава России (г. Новосибирск) не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронно.

2.3 Порядок защиты персональных данных.

2.3.1 Защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена ФГБУ «ФЦН» Минздрава России (г. Новосибирск) за счет его средств в порядке, установленном федеральными законами Российской Федерации в области защиты персональных данных.

2.3.2 ФГБУ «ФЦН» Минздрава России (г. Новосибирск) обязана при обработке персональных данных субъектов персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2.3.3 Соблюдать порядок получения, учета и хранения персональных данных субъектов ПДн.

2.3.4 Применять технические средства охраны и сигнализации.

2.3.5 Взять со всех работников, связанных с получением, обработкой и защитой

персональных данных субъектов ПДн, типовое обязательство сотрудника ФГБУ «ФЦН» Минздрава России (г. Новосибирск) о неразглашении информации, содержащей персональные данные.

2.3.6 Привлекать к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн.

2.3.7 Запретить допуск к персональным данным субъектов ПДн работников ФГБУ «ФЦН» Минздрава России (г. Новосибирск), не включенных в Перечень лиц, допущенных к обработке персональных данных, обрабатываемых в ИСПДн ФГБУ «ФЦН» Минздрава России (г. Новосибирск).

2.3.8 Защита доступа к электронной базе данных, содержащей персональные данные субъектов ПДн, должна обеспечиваться путем использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн.

2.3.9 Копировать и делать выписки персональных данных субъектов ПДн разрешается исключительно в служебных целях с письменного разрешения руководителя.

2.3.10 Субъекты ПДн не должны отказываться от прав на сохранение и защиту своих персональных данных.

2.3.11 ФГБУ «ФЦН» Минздрава России (г. Новосибирск), субъекты ПДн и их представители должны совместно вырабатывать меры защиты персональных данных субъектов ПДн.

3 Хранение персональных данных

3.1 Сведения о субъектах ПДн в ФГБУ «ФЦН» Минздрава России (г. Новосибирск) на бумажных носителях должны храниться в специально оборудованных шкафах и сейфах, которые запираются и опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у ответственных сотрудников.

3.2 Обязанности по хранению сведений о субъектах ПДн, заполнению, хранению и выдаче документов, содержащих персональные данные, в ИСПДн возлагаются на Ответственного за обработку и защиту персональных данных.

3.3 Съёмные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПДн, должны быть промаркированы и учтены в журнале регистрации, учета и выдачи внешних носителей для хранения резервных копий ПДн.

3.4 В процессе хранения персональных данных субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4 Передача персональных данных

4.1 При передаче персональных данных субъекта ПДн ФГБУ «ФЦН» Минздрава России (г. Новосибирск) должна соблюдаться следующие требования:

4.1.1 Передавать персональные данные субъекта ПДн представителю субъекта ПДн в порядке, установленном федеральными законами Российской Федерации.

5 Уничтожение персональных данных

5.1 При необходимости уничтожения персональных данных ФГБУ «ФЦН» Минздрава России (г. Новосибирск) должна руководствоваться следующими требованиями:

5.1.1 Уничтожение персональных данных в ИСПДн осуществляется комиссией по проведению мероприятий по защите персональных данных.

5.1.2 Бумажные носители персональных данных должны уничтожаться при помощи специального оборудования (измельчителя бумаги).

5.1.3 Персональные данные, представленные в электронном виде, должны уничтожаться специализированным программным обеспечением, гарантирующим предотвращение восстановления удаленных данных.

5.1.4 После окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

6 Внутренние проверки состояния защищенности информационной системы персональных данных

6.1 Проверка состояния защищенности ИСПДн осуществляется комиссией по проведению мероприятий по защите персональных данных.

6.2 Проверка состояния защищенности ИСПДн осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых ФГБУ «ФЦН» Минздрава России (г. Новосибирск), требованиям законов и иных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты персональных данных.

6.3 Проверка состояния защищенности ИСПДн включает в себя:

6.3.1 Определение характера циркулирующих персональных данных и установленных в ИСПДн режимов их обработки.

6.3.2 Определение актуальности организационно-распорядительной документации, учитывающей конкретные условия функционирования средств вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты информации), порядок работы сотрудников организации при эксплуатации средств вычислительной техники.

6.3.3 Анализ принятых мер (программных, технических, организационных), обеспечивающих защиту средств вычислительной техники, информационной системы и баз данных от несанкционированного доступа, оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов соответствия).

6.3.4 Проверка наличия лицензионных средств защиты от вредоносных программ и вирусов или сертифицированных свободно распространяемых антивирусных средств защиты.

6.3.5 Проверка состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва).

6.3.6 Проверка состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

6.4 Внутренняя проверка Комиссии по проведению мероприятий по защите персональных данных завершается подведением итогов (обобщением) результатов проверки и составлением акта о результате проверки состояния защищенности ИСПДн.

6.5 Акт должен содержать:

6.5.1 Дата, время и место составления акта.

6.5.2 Дата и место проведения проверки.

6.5.3 Сведения о результатах проверки, в том числе о выявленных нарушениях и их характере.

6.5.4 Достоверное и обоснованное изложение состояния защищенности информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков.

7 Обязанности субъекта персональных данных и Оператора

7.1 В целях обеспечения достоверности персональных данных субъект ПДн обязан:

7.1.1 Предоставлять ФГБУ «ФЦН» Минздрава России (г. Новосибирск) полные и достоверные данные о себе.

7.1.2 В случае изменения своих персональных данных сообщать данную информацию ФГБУ «ФЦН» Минздрава России (г. Новосибирск).

7.2 ФГБУ «ФЦН» Минздрава России (г. Новосибирск) обязан:

7.2.1 Осуществлять защиту персональных данных субъекта ПДн.

7.2.2 Вести Журнал учета обращений субъектов персональных данных по вопросам обработки их ПДн в ИСПДн ФГБУ «ФЦН» Минздрава России (г. Новосибирск) (Приложение №2 к Положению).

7.2.3 Обеспечивать хранение документации, содержащей персональные данные субъектов ПДн, 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.

8 Права субъекта ПДн в целях защиты персональных данных

8.1 Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения (Приложение №3 к Положению).

8.3 Субъект персональных данных имеет право на определение представителей для защиты своих персональных данных.

8.4 Субъект персональных данных имеет право требовать исключить или исправить неверные или неполные персональные данные, а также данные, обрабатываемые с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8.5 Субъект персональных данных имеет право требовать об извещении ФГБУ «ФЦН» Минздрава России (г. Новосибирск) всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.6 Субъект персональных данных имеет право на обжалование в судебном порядке любых неправомерных действий или бездействия ФГБУ «ФЦН» Минздрава России (г. Новосибирск) при обработке и защите его персональных данных.

9 Реагирование на запросы субъектов ПДн и их законных представителей

9.1 При рассмотрении запросов, поступающих от субъектов ПДн и их законных представителей, ФГБУ «ФЦН» Минздрава России (г. Новосибирск) руководствуется Правилами рассмотрения запросов (Приложение №4 к Положению).

9.2 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 (Приложение №5 и №6 к Положению).

10 Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

10.1 Лица, виновные в нарушении требований федеральных законов РФ, несут предусмотренную законодательством РФ ответственность.

10.2 Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.