

УТВЕРЖДАЮ



Главный врач
Н.А. Семашко»

Л.Ю. Сорокина
01.01.2012 г.

ПОЛОЖЕНИЕ

о ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ
в Государственном бюджетном учреждении Рязанской области
«Клиническая больница им Н.А. Семашко»

СОДЕРЖАНИЕ.

1. Введение.....	стр. 3
1.1. Правовая база Положения о защите персональных данных пациентов в ГБУ РО «КБ им. Н.А. Семашко».....	стр. 5
2. Основные понятия.....	стр. 7
3. Основные условия проведения обработки персональных данных пациентов в ГБУ РО «КБ им. Н.А. Семашко».....	стр. 16
4. Обязанности оператора обработки, использования и хранения персональных данных пациентов в ГБУ РО «КБ им. Н.А. Семашко»	стр. 19
4.1. Получение согласия субъекта на обработку его персональных данных.	
4.2. Использование и хранение персональных данных пациентов в ГБУ РО «КБ им. Н.А. Семашко».	
4.3. Передача персональных данных пациентов в ГБУ РО «КБ им. Н.А. Семашко».	
4.4. Обмен персональных данных пациентов.	
5. Права субъекта персональных данных.....	стр. 24
6. Идентификация субъектов персональных данных. Персонифицированные и деперсонифицированные данные субъектов персональных данных.....	стр. 26
7. Первичные и вторичные медицинские данные субъектов персональных данных.....	стр. 28
8. Последствия неисполнения Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных».....	стр. 29
9. Приложения:	стр. 32
<i>Приложение № 1: «Журнал учета обращений пациентов - субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационных системах персональных данных пациентов ГБУ РО «КБ им. Н.А. Семашко» на трёх (3) листах.</i>	
<i>Приложение № 2: «Письменное согласие пациента на обработку его персональных данных. Согласие на обработку персональных данных» на двух (2) листах.</i>	
10. Лист согласования.....	стр. 39

ВВЕДЕНИЕ.

Настоящее Положение о защите персональных данных пациентов в ГБУ РО «КБ им. Н.А. Семашко» (далее «Положение») разработано в ГБУ РО «КБ им. Н.А. Семашко», является официальным документом, в котором определено обеспечение информационной безопасности пациентов ГБУ РО «КБ им. Н.А. Семашко», защита конфиденциальной информации в сфере медицинской деятельности ГБУ РО «КБ им. Н.А. Семашко».

Необходимость разработки «Положения» обусловлена требованиями Федерального закона № 152-ФЗ от 27.07.2006 года «О персональных данных».

Настоящее «Положение» определяет основные цели и задачи **системы защиты персональных данных (СЗПДн)** пациентов в ГБУ РО «КБ им. Н.А. Семашко». «Положение» определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

«Положение» разработано в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты **персональных данных пациентов (ПДнП)**, с позиции комплексного применения технических и организационных мер и средств защиты.

Под **информационной безопасностью персональных данных пациентов** понимается защищённость персональных данных пациентов и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

«Положение» является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ПДн пациентов в **информационных системах персональных данных пациентов (ИСПДНП)** в ГБУ РО «КБ им. Н.А. Семашко»;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление,

отражение и ликвидацию последствий реализации различных видов угроз ПДн пациентов.;

- координацию деятельности структурных подразделений ГБУ РО «КБ им. Н.А. Семашко» при проведении работ по развитию и эксплуатации ИСПДнП с соблюдением требований обеспечения безопасности ПДнП;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДнП в ИСПДнП в ГБУ РО «КБ им. Н.А. Семашко».

Область применения «Положения» распространяется на все структурные подразделения ГБУ РО «КБ им. Н.А. Семашко», эксплуатирующие технические и программные средства ИСПДнП, в которых осуществляется автоматизированная обработка ПДнП, а также на все структурные подразделения ГБУ РО «КБ им. Н.А. Семашко», осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДнП в ГБУ РО «КБ им. Н.А. Семашко».

ПРАВОВАЯ БАЗА
ПОЛОЖЕНИЯ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ В
ГБУ РО «Клиническая больница им. Н.А. Семашко».

Правовой базой для разработки настоящего «Положения» служат требования следующих действующих в России законодательных и нормативных документов, регламентирующих требования к организации обеспечения безопасности персональных данных в медицинских организациях:

- Конституция Российской Федерации (принята 12.12.1993, ред. от 21.07.07. № 5-ФЗ), ст. 23,24 (*Неприкосновенность частной жизни, Личная и семейная тайна*), ст. 41,42 (*Недопустимость сокрытия информации, связанной с угрозой жизни и здоровью*);
- Закон РФ от 28 июля 1991 г. № 1499-1 «О медицинском страховании граждан в Российской Федерации» (в ред. от 29.12.06. № 258-ФЗ), ст. 12 – «*Ведение баз данных*»;
- ФЗ РФ от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в РФ» (далее - "Основы..."); статьи 13, 22, 78, 79, 91) в статье 13 "Основ..." дано определение врачебной тайны, как «*сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении*»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в котором даны определения понятий: информация, документирование информации, защита информации, обладатель информации, конфиденциальность информации, предоставление и распространение информации, электронное сообщение;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), в котором регулируются отношения, связанные с обработкой персональных данных с использованием средств автоматизации;
- Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изм. и доп.), в котором в котором к указанной категории информации отнесены персональные данные и сведения, содержащие врачебную тайну;
- Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», в котором определены основные требования к указанным информационным системам (ИС).

Основные требования к организации защиты информации в учреждениях изложены в государственных стандартах:

- ГОСТ Р ИСО/МЭК 15408-1,2,3-2002 Критерии оценки безопасности информационных технологий. Функциональные требования безопасности.
- ГОСТ Р ИСО/МЭК ТО 13335-5-2006, 13335-1,3,4-2007 Информационная технология. Методы и средства обеспечения безопасности.
- ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ОСНОВНЫЕ ПОНЯТИЯ.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения

персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Персональные данные (ПДн) – любая информация, связанная с физическим лицом (субъектом ПДн), позволяющая идентифицировать конкретное физическое лицо среди прочих лиц.

Персональные данные пациента – информация, необходимая больнице для выполнения договора об оказании медицинских услуг пациенту (субъекту ПДн) и касающаяся этого конкретного физического лица, которое предоставляет свои ПДн для обработки медицинской организации.

К персональным данным пациента (ПДнП) относятся любые сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Общие категории ПДнП – Ф.И.О., дата и место рождения, адрес проживания, профессия, сведения о состоянии здоровья, интимной жизни.

Общие категории ПДнП следует отличать от общедоступных ПДнП, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальная информация не подлежит передаче третьим лицам без согласия её обладателя.

Обладателем конфиденциальной информации является лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать к ней доступ на основании закона или договора.

Применительно к информации, содержащей врачебную тайну, её обладателем является пациент или его законный представитель, следовательно должно быть получено согласие пациента на передачу касающихся его сведений, содержащих врачебную тайну, кому-либо, в том числе должностным лицам в интересах его обследования и лечения (статья 13 «Основ...»).

Обработкой персональных данных является любое из следующих действий: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передача), обезличивание, блокирование, уничтожение персональных данных.

Обработка ПДнП проводится в связи с обращениями пациентов в ЛПУ в целях установления диагноза, оказания медицинских и медико-социальных услуг в рамках ОМС, ДМС, для оказания платных медицинских услуг при условии, что обработка ПДнП осуществляется лицом, профессионально

занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну.

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

Доступ к информации – возможность получения информации и её использования.

Доступ в операционную среду компьютера (информационной системы персональных данных пациентов - ИСПДнП) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожение, копирование, перемещение и т.п.), исполняемых файлов прикладных программ.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным и документам.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная 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.

Информационная система персональных данных (ИСПДн) ГБУ РО «КБ им. Н.А. Семашко» относится к 1 классу (К1) информационных систем (все ИС, в которых обрабатывается информация ПДн 1-й категории), для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных (СПДн). К такой ИСПДн предъявляются повышенные требования по обеспечению их безопасности.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Обработка персональных данных, содержащихся в ИСПДнП либо извлечённых из такой системы, считается осуществлённой без использования средств автоматизации (*неавтоматизированной*), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов персональных данных, осуществляется при непосредственном участии человека.

Персональные данные пациентов при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных.

Обработка ПДнП, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДнП можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДнП либо имеющих к ним доступ.

При хранении материальных носителей ПДнП должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение

информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности 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.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Электронная персональная медицинская запись (ЭПМЗ) – это любая запись, сделанная конкретным медицинским работником в отношении конкретного пациента, сохранённая на электронном носителе.

ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ
ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ
в ГБУ РО «КБ им. Н.А. Семашко».

1. ГБУ РО «КБ им. Н.А. Семашко» - ОПЕРАТОР, производящий обработку персональных данных пациентов (ПДнП) определяет объём, содержание обрабатываемых ПДнП, руководствуясь нормативно-правовыми актами, регламентирующими требования к организации обработки ПДнП в медицинских организациях.

Медицинские информационные системы относятся к специальным системам, поскольку в них обрабатываются данные о состоянии здоровья пациентов.

2. Для обработки персональных данных, относимых к общим категориям, обязательно наличие согласия на это субъекта персональных данных.

3. При отсутствии согласия субъекта обработка общих категорий персональных данных допускается в случае, если:

- она осуществляется на основании и во исполнение федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора, т. е. правовым основанием для такой обработки всегда должен являться федеральный закон;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных, т. е. в качестве основания для обработки выступает договор, заключенный между субъектом персональных данных и оператором, который косвенно (но не прямо! – если такого положения не содержится в условиях заключенного договора) подтверждает согласие субъекта на обработку таких данных;
- обработка персональных данных осуществляется в статистических или иных научных целях при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта

персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услуг связи;
- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в т. ч. персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

4. В отношении специальных категорий персональных данных пациентов в соответствии с Законом № 152-ФЗ **обработка специальных категорий допускается в случае, если:**

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных. В данном условии и заключается коллизия: согласия субъекта достаточно как для обработки общих персональных данных, так и для обработки специальных персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта персональных данных, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка данных производится лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующим общественным объединением или религиозной организацией, действующими в соответствии с законодательством РФ, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут

- распространяться без согласия в письменной форме субъектов персональных данных;
- обработка персональных данных необходима в связи с осуществлением правосудия;
 - обработка персональных данных осуществляется в соответствии с законодательством РФ о безопасности, оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

Персональные данные для обработки предоставляют субъекты персональных данных – пациенты ГБУ РО «КБ им. Н.А. Семашко».

5. Если ПДнП необходимо получить у третьей стороны, то оператор ПДнП обязан заранее уведомить об этом пациента (субъекта ПДн) и получить его письменное согласие. Оператор ПДнП должен сообщить пациенту о целях, предполагаемых источниках и способах получения ПДнП, а также характере подлежащих получению ПДнП и последствиях отказа пациента (субъекта ПДн) дать письменное согласие на их получение.

6. Субъекты персональных данных и их законные представители могут быть ознакомлены под роспись с настоящим «Положением о защите персональных данных пациентов в ГБУ РО «КБ им. Н.А. Семашко», устанавливающим порядок обработки ПДнП, а также их правах и обязанностях в этой области. С этой целью в больнице организуется и ведётся Журнал учёта обращений пациентов – субъектов персональных данных о выполнении их законных прав при обработке ПДнП в ИСПДнП в ГБУ РО «КБ им. Н.А. Семашко».

Форма «Журнала учёта обращений пациентов – субъектов персональных данных о выполнении их законных прав при обработке ПДнП в ИСПДнП в ГБУ РО «КБ им. Н.А. Семашко» утверждается приказом главного врача.

7. Приказ Министерства здравоохранения и социального развития РФ от 22.11.2004 г. № 255 регламентирует хранение и выдачу медицинских карт. Медицинская карта амбулаторного больного хранится в регистратуре поликлиники. Поскольку карта является юридическим документом, она не должна выдаваться на руки пациенту. Но в соответствии со ст. 22 ФЗ РФ № 323-ФЗ «Об основах охраны здоровья граждан в РФ» пациент имеет право непосредственно знакомиться с медицинской документацией, отражающей состояние его здоровья, и получать консультации по ней у других специалистов. По требованию пациента ему должны предоставляться копии медицинских документов, если в них не затрагиваются интересы третьей стороны. Все необходимые выписки из медицинской карты делает лечащий врач. Пациент может получить медицинскую карту на руки, чтобы на месте ознакомиться с документом. Выдача данного документа на руки пациенту

возможна только с разрешения главного врача и лично тому человеку, чьё имя указано на карте. Факт обращения пациента – субъекта персональных данных о выполнении его законных прав при обработке ПДн в ИСПДнП в ГБУ РО «КБ им. Н.А. Семашко» фиксируется в Журнале обращений пациентов. Таким образом, действующее законодательство позволяет пациенту накапливать копии всех медицинских документов.

ОБЯЗАННОСТИ ОПЕРАТОРА

ОБРАБОТКИ, ИСПОЛЬЗОВАНИЯ и ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ в ГБУ РО «КБ им. Н.А. Семашко».

Обработку персональных данных осуществляют операторы. Законом № 152-ФЗ установлено, что оператор – это государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

ПОЛУЧЕНИЕ СОГЛАСИЯ СУБЪЕКТА

на ОБРАБОТКУ его ПЕРСОНАЛЬНЫХ ДАННЫХ.

Законом установлено, что оператор, осуществляющий обработку персональных данных (в данном случае ЛПУ), обязан предоставить доказательство согласия субъекта на обработку его персональных данных («Письменное согласие пациента на обработку его персональных данных»). Таким образом, устанавливается презумпция вины оператора, и в случае несоблюдения им обязанности получить данное согласие риски несет медицинская организация.

Субъект персональных данных сам принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку своей волей и в своём интересе, за исключением случаев, когда предусматривается обязательное их предоставление в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. За исключением последнего, согласие на обработку персональных данных может быть отозвано субъектом персональных данных (ст. 9 Закона РФ № 152-ФЗ).

Документ, фиксирующий факт получения согласия субъекта персональных данных, включает в себя:

- фамилию, имя, отчество, адрес пациента, номер основного документа, удостоверяющего его личность, сведения о дате его выдачи и выдавшем органе;
- наименование и адрес оператора обработки персональных данных;

- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие пациента;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

При отказе пациента (для ОМС – застрахованного лица) оформить письменное согласие на обработку его ПДн, необходимо доказать, что при оказании услуг медицинской помощи, предусмотренной программой государственных гарантий гражданам на бесплатную медицинскую помощь, оформление этого документа должно быть обязательным, за исключением случаев, предусмотренных законодательством РФ, когда такое согласие необязательно. Для обработки персональных данных, относимых к общим категориям, обязательно наличие согласия на это субъекта персональных данных.

При отсутствии согласия субъекта обработка общих категорий персональных данных допускается в случае, если:

- она осуществляется на основании и во исполнение федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора, т. е. правовым основанием для такой обработки всегда должен являться федеральный закон;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных, т. е. в качестве основания для обработки выступает договор, заключенный между субъектом персональных данных и оператором, который косвенно (но не прямо! – если такого положения не содержится в условиях заключенного договора) подтверждает согласие субъекта на обработку таких данных;
- обработка персональных данных осуществляется в статистических или иных научных целях при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за

оказанные услуги связи, а также для рассмотрения претензий пользователей услуг связи;

- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в т. ч. персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

В соответствии с Законом № 152-ФЗ **обработка специальных категорий допускается в случае, если:**

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта персональных данных, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка данных производится лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующим общественным объединением или религиозной организацией, действующими в соответствии с законодательством РФ, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;
- обработка персональных данных необходима в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством РФ о безопасности, оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

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

- подтверждение факта обработки персональных данных оператором, а также цель данной обработки;
- способы обработки персональных данных, применяемые оператором;
- 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 т. ч. сроки их хранения;
- сведения о том, какие юридические последствия для субъекта может повлечь за собой обработка его персональных данных;
- разъяснения последствий его отказа в предоставлении своих персональных данных в случае, если это установлено в качестве обязанности субъекта федеральным законом.

Если персональные данные были получены не от субъекта персональных данных, оператор до начала их обработки обязан предоставить субъекту следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя, от которого были получены данные;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные права субъекта персональных данных.

ИСПОЛЬЗОВАНИЕ и ХРАНЕНИЯ

ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ.

ПДнП в ГБУ РО «КБ им. Н.А. Семашко» обрабатываются и хранятся на бумажных и электронных носителях в специально для этого предназначенных помещениях.

В процессе обработки и хранения ПДнП должно обеспечиваться :

- требования нормативно-правовых актов соблюдения конфиденциальности любой информации о пациентах;
- конфиденциальность ПДн – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания для такого распространения;
- сохранность имеющихся ИСПДнП, ограничение доступа к ним в соответствии с законодательством РФ и настоящим «Положением».

Доступ к информационным системам персональных данных пациентов имеют:

- главный врач;
- заместители главного врача;
- главная медицинская сестра;
- руководители структурных подразделений;
- врачи и медицинские сёстры данных структурных подразделений
- лечащие врачи субъектов ПДн;
- медрегистраторы;
- сотрудники кабинета медицинской статистики;
- сотрудники оперативного отдела;
- сотрудники архива ПДнП;
- сотрудники клинических кафедр РГМУ им. акад. И.П. Павлова в соответствии с договором ГБУ РО «КБ им. Н.А. Семашко» и РГМУ им. акад. И.П. Павлова «О совместном сотрудничестве и безвозмездном использовании учебных площадей»;
- органы управления здравоохранением;
- надзорно-контрольные органы;
- страховые организации и фонды ОМС;
- научно-исследовательские учреждения и т.д.

ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ.

С согласия гражданина или его законного представителя допускается передача сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в интересах обследования и лечения пациента, для проведения научных исследований, публикаций в научной литературе, использования этих сведений в учебном процессе и в иных целях.

Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

- 1) в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;
- 2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- 3) по запросу органов дознания и следствия и суда в связи с проведением расследования или судебным разбирательством;
- 4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с п. 2 ч. 2 ст. 20 ФЗ РФ № 323-ФЗ «Об основах..», а также несовершеннолетнему, не достигшему возраста, установленного ч. 2 ст. 54 настоящего ФЗ, для информирования одного из его родителей или иного законного представителя;
- 5) при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий;
- 6) в целях проведения военно-врачебной экспертизы в порядке, установленном положением о военно-врачебной экспертизе, утвержденным Правительством Российской Федерации.

ОБМЕН ПЕРСОНАЛЬНЫМИ ДАННЫМИ ПАЦИЕНТОВ.

Обмен ПДнП при их обработке в ИСПДнП осуществляется по каналам связи, защита которых обеспечивается при реализации соответствующих организационных мер и (или) путём применения технических средств. Размещение ИС, специальное оборудование и охрана помещений, в которых ведётся работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

Субъект персональных данных в соответствии с Законом № 152-ФЗ обладает следующими правами:

- получения сведений об операторе, месте его нахождения, наличии у оператора персональных данных, относящихся к субъекту, правом ознакомления с такими персональными данными;
- требования от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели

обработки, а также принятия предусмотренных законом мер по защите своих прав;

- на предоставление оператором сведений о наличии ПДн в доступной форме;
- на доступ к ПДн данным законного представителя субъекта на основании запроса. Термин “законный представитель” расшифровывается в ст. 26 Гражданского кодекса РФ (это родители, усыновители или попечитель лица в возрасте от 14 до 18 лет). При необходимости оказания медицинской помощи лицу, не достигшему возраста совершеннолетия, перед ЛПУ встает ряд вопросов, касающихся участия в данном процессе его законного представителя. Зачастую сотрудниками ЛПУ неверно трактуется понятие законного представителя, и под ним понимается лицо, которому пациент доверяет информацию о факте его обращения за медицинской помощью, состоянии здоровья, диагнозе заболевания и иные сведения, полученные при его обследовании и лечении в силу ст. 13, 20, 22 Основ. Тем не менее, статус законного представителя иной: он вправе осуществлять от имени представляемого любые действия, в т. ч. и определять, кому будет разглашена информация, составляющая врачебную тайну пациента. У лица же, которому могут быть переданы сведения, составляющие врачебную тайну, никаких прав по вступлению в гражданские правоотношения от имени пациента нет.)
- на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в т. ч. содержащей:

– подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

– способы обработки персональных данных, применяемые оператором;

– 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 т. ч. сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Обработка персональных данных в ЛПУ должна осуществляться с соблюдением необходимых, но разумных мер, обеспечивающих конфиденциальность информации и ее защиту от несанкционированного доступа. Конфиденциальность персональных данных – это обязательное для

соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания для такого распространения. Статьей 13 Основ устанавливаются законные основания для нарушения условия конфиденциальности, и, на наш взгляд, дополнительные меры защиты информации являются в ряде случаев излишними.

Кроме того, ст. 7 Закона № 152-ФЗ установлено, что обеспечение конфиденциальности персональных данных не требуется в случае их обезличивания и в отношении общедоступных персональных данных.

ИДЕНТИФИКАЦИЯ ПАЦИЕНТОВ.

ПЕРСОНИФИЦИРОВАННЫЕ и ДЕПЕРСОНИФИЦИРОВАННЫЕ ДАННЫЕ ПАЦИЕНТОВ.

Идентификатор пациента – уникальный символьный или цифровой код, применяемый для обозначения пациента и относящихся к нему данных в определённой учётной системе (системе учёта).

Медицинские данные пациента – сведения о физиологических особенностях организма, перенесённых заболеваниях, состоянии здоровья и (или) оказанной пациенту медицинской помощи.

Персонифицированные данные – совокупность сведений, включающая персональные данные пациента, которые позволяют идентифицировать его личность.

Обезличивание данных пациента – действия по удалению персональных данных пациента, в результате которого ни при каких условиях невозможно определить принадлежность медицинских данных конкретному физическому лицу и идентифицировать его личность. Обезличенные данные не являются конфиденциальными. Обезличивание данных используется в тех случаях, когда не требуется сопоставление медицинских данных с конкретным пациентом, например, для их статистической обработки, научных и учебных целей и т.д.

Анонимизация данных – использование для обозначения (пометки) медицинских данных (документов), относящихся к некоторому пациенту, его условного имени – *КРИПТОНИМА* (от греч. «kryptos» - тайный, скрытый и «опута» - имя), раскрытие которого возможно только самим пациентом. Предполагается, что при использовании криптонима для идентификации пациента его персональные данные пациента в учётной системе не хранятся. Ответственность за раскрытие своего криптонима несёт только сам пациент. Анонимные данные не являются конфиденциальными, поэтому согласия

пациента на их обработку не требуется. Анонимизация данных используется, в частности, в тех случаях, когда сам пациент организует сбор, накопление и передачу на хранение своих медицинских данных, например, на серверах в сети Интернет, а также при анонимном лечении.

Псевдонимизация данных – совокупность организационно-технических мероприятий, процедур и действий по присвоению пациенту специального *ПСЕВДОНИМА* (от греч. «pseudo» - ложный и «онума» - имя) для передачи, сбора, хранения и обработки его медицинских данных, исключающая возможность его несанкционированного сопоставления с конкретным физическим лицом и идентификацию его личности. Формирование псевдонима и его обратное сопоставление с персональными данными пациента осуществляется с помощью криптографических средств, использование которых жёстко регламентировано.

Псевдоним: а) никогда не указывается на медицинских и иных документах, содержащих персональные данные пациента; б) во всех случаях не известен пациенту и поэтому не может быть им раскрыт или передан кому-либо (в отличие от других его идентификаторов, например, страховой номер индивидуального страхового счёта; в) может быть сопоставлен с персональными данными пациента (дешифрован) только с согласия пациента либо в иных случаях, предусмотренных законодательством; г) персональный перечень должностных лиц, которым в этих случаях стала известна информация о соответствии псевдонима конкретному пациенту (его ПДн), строго определён и также известен. Псевдонимизированные данные не содержат ПДнП и в этом смысле уже не являются конфиденциальными, что позволяет осуществлять их обработку без согласия пациентов. Псевдонимизация персонифицированных сведений целесообразна при организации «сводных» медицинских баз данных (МБД), когда:

а) круг пользователей МБД достаточно широк (например, органы управления здравоохранением, надзорно-контрольные органы, страховые организации и фонды ОМС, научно-исследовательские учреждения и т.д.);

б) возможны случаи, когда в процессе обработки и анализа ПДнП может возникнуть необходимость идентификации его личности или непосредственного контакта с ним, например, должностных лиц надзорно-контрольных органов.

Примерами подобных псевдонимизированных МБД могут являться специализированные медицинские регистры: доноров, онкологический, диабетический и т.п.

Принципиально важным является то, что пользователям псевдонимизированных МБД какие-либо криптографические средства для

обработки псевдонимов не нужны. При этом значительно снижаются требования к средствам защиты таких баз данных.

Иногда псевдонимизацией данных называют также их анонимное представление – без указания ПДнП, вместо которых используется его криптоним.

ПОЛИЦЕВЫЕ данные – совокупность данных, относящихся к некоторому физическому лицу (пациенту). В зависимости от наличия в их составе ПДнП и используемых идентификаторов пациентов полицейские данные могут быть: *а) персонифицированными, б) псевдонимизированными, в) анонимными, г) обезличенными.*

ПЕРВИЧНЫЕ И ВТОРИЧНЫЕ МЕДИЦИНСКИЕ ДАННЫЕ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.

«Полицейские» медицинские данные, их потоки и хранилища (базы данных) разделяются на две категории:

1. **ПЕРВИЧНЫЕ ДАННЫЕ**, которые формируются и используются медицинскими работниками непосредственно в процессе оказания медицинской помощи пациенту и при ведении электронной медицинской карты в больнице.

Доступ к персонифицированным первичным данным строго ограничен и жестко регламентирован законодательством.

2. **ВТОРИЧНЫЕ ДАННЫЕ** – интегрированные, агрегированные полицейские медицинские данные, формируемые на основе первичных данных, поступающих из множества лечебных учреждений. Обычно такие данные накапливаются в течение продолжительного времени в виде различных «сводных» МБД, используемых органами управления для анализа, планирования, выполнения надзорно-контрольных функций, ведения «листов ожидания», а также экспертизы, оплаты (клиринга), эпидемиологических и иных научных исследований и т.д. пользователи таких МБД, как правило, непосредственно не оказывают медицинскую помощь пациентам.

ПОСЛЕДСТВИЯ НЕИСПОЛНЕНИЯ

ЗАКОНА «О ПЕРСОНАЛЬНЫХ ДАННЫХ».

В соответствии со статьёй 24 Федерального закона №152-ФЗ «Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную и иную, предусмотренную законодательством Российской Федерации ответственность».

Преступлениями, за совершение которых предусмотрена уголовная ответственность, являются:

- **статья 137 УК РФ – «Нарушение неприкосновенности частной жизни»**
 - незаконные сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации;

- **статья 140 УК РФ – «Отказ в предоставлении гражданину информации»**
 - неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан;

- **статья 272 УК РФ – «Неправомерный доступ к компьютерной информации»**
 - неправомерный доступ к охраняемой законом компьютерной информации, содержащейся на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокировку, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

- **статья 183 УК РФ – «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»;**
- **статья 273 УК РФ – «Создание, использование и распространение вредоносных программ для ЭВМ»;**
- **статья 274 УК РФ – «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»;**
- **статья 292 УК РФ – «Служебный подлог»;**
- **статья 293 УК РФ – «Халатность».**

Административная ответственность.

Административная ответственность (предупреждения, штрафы для граждан, должностных лиц и юридических лиц, конфискация средств защиты информации, административное приостановление деятельности) может наступить по следующим статьям:

- Статья 5.27 КОАП РФ «Нарушение законодательства о труде и об охране труда»;
- Статья 5.39 КОАП РФ «Отказ в предоставлении гражданину информации»;
- Статья 13.11 КОАП РФ «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных);»;
- Статья 13.12 КОАП РФ «Нарушение правил защиты информации»;
- Статья 13.13 КОАП РФ «Незаконная деятельность в области защиты информации»;
- Статья 13.14 КОАП РФ «Разглашение информации с ограниченным доступом»;
- Статья 13.19 КОАП РФ «Нарушение порядка представления статистической информации»;
- Статья 19.4 КОАП РФ «Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль)»;
- Статья 19.5 КОАП РФ «Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)»;
- Статья 19.6 КОАП РФ «Непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения»;
- Статья 19.7 КОАП РФ «Непредставление сведений (информации)»;

- Статья 19.20 КОАП РФ «Осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии)»;
- Статья 20.25 КОАП РФ «Неуплата административного штрафа либо самовольное оставление места отбывания административного ареста»;
- Статья 32.2 КОАП РФ «Исполнение постановления о наложении административного штрафа».

ПРИЛОЖЕНИЯ:

Приложение № 1:

«Журнал учета обращений пациентов - субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационных системах персональных данных пациентов ГБУ РО «КБ им. Н.А. Семашко» на трёх (3) листах.

Приложение № 2:

«Письменное согласие пациента на обработку его персональных данных. Согласие на обработку персональных данных» на двух (2) листах.

Государственное бюджетное учреждение Рязанской области
«Клиническая больница им. Н.А. Семашко»

УТВЕРЖДАЮ

Главный врач
ГБУ РО «КБ им. Н.А. Семашко»

Л.Ю. Сорокина
01.01.2012 г.



Журнал учета

обращений пациентов - субъектов персональных данных
о выполнении их законных прав, при обработке персональных
данных в информационных системах персональных данных
пациентов ГБУ РО «КБ им. Н.А. Семашко»

ОБРАЗЕЦ ЗАПОЛНЕНИЯ

№	ФИО	Дата	Цель	Ответственный за выдачу информации
	<i>Иванов И.И.</i>	<i>01.10.2010</i>	<i>Информирование</i>	
	<i>Сидоров С.С.</i>	<i>01.10.2010</i>	<i>Прекращение обработки</i>	
	<i>Петров П.П.</i>	<i>01.10.2010</i>	<i>Уточнение персональных данных</i>	

УТВЕРЖДАЮ

 ГБУ РО «КБ им. Н.А. Семашко»
Л.Ю. Сорокина

ГБУ РО «Клиническая больница им. НА. Семашко»

Письменное согласие пациента на обработку его персональных данных.

Согласие на обработку персональных данных.

Я, нижеподписавшийся, _____

(Ф.И.О.. полностью)

проживающий по адресу _____

(по месту регистрации)

паспорт _____

(серия, номер, дата выдачи, название выдавшего органа)

сам принимаю решение о предоставлении своих персональных данных и даю согласие на их обработку своей волей и своим интересом, за исключением случаев, когда предусматривается обязательное их предоставление в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов других лиц, обеспечение обороны и безопасности России.

В соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. «О персональных данных» № 152-ФЗ подтверждаю своё согласие на обработку ГБУ РО «КБ им. Н.А. Семашко»; 390005, г. Рязань, ул. Семашко, д.3; тел./факс: (4912) 76-57-23; E-mail: kbsemashko@yandex.ru (далее - Оператор) моих персональных данных, включающих: фамилию, имя, отчество, пол, дату рождения, адрес проживания, контактный телефон, реквизиты полиса ОМС (ДМС), страховой номер Индивидуального лицевого счёта в Пенсионном фонде России (СНИЛС), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания Оператором мне медицинской помощи я предоставляю право медицинским работникам передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчётные формы, предусмотренные документами, регламентирующими предоставление отчётных данных (документов) по ОМС (договором ДМС).

Оператор имеет право во исполнение своих обязательств по работе в системе ОМС (по договору _____ ДМС _____ на обмен (приём и передачу) моими персональными данными со страховой медицинской организацией

_____ (название) и территориальным фондом ОМС с использованием машинных носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их приём и обработка будут осуществляться лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов и составляет двадцать пять лет (для стационара), пять лет (для поликлиники).

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия:

- я разрешаю, не разрешаю (*нужное подчеркнуть*) передавать следующие мои персональные данные через справочное бюро Оператора: мои фамилия, имя, отчество, наименование отделения, где я лечусь;

- я разрешаю, не разрешаю (*нужное подчеркнуть*) моему лечащему врачу, заведующему отделением, где я лечусь, передавать мои персональные данные (сведения о моём заболевании, лечении, прогнозе заболевания) моим родителям, жене, мужу, совершеннолетним детям и иному моему законному представителю

(термин "законный представитель" расшифровывается в ст. 26 Гражданского кодекса РФ (это родители, усыновители или попечитель лица в возрасте от 14 до 18 лет)).

Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

- 1) в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;
- 2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- 3) по запросу органов дознания и следствия и суда в связи с проведением расследования или судебным разбирательством;
- 4) в случае оказания помощи несовершеннолетнему в возрасте, установленном ст. 13, п. 2 ч. 2 ст. 20 и ч. 2 ст. 54 ФЗ № 323 ФЗ, для информирования его родителей или законных представителей;
- 5) при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий;

б) в целях проведения военно-врачебной экспертизы в порядке, установленном положением о военно-врачебной экспертизе, утверждаемым Правительством Российской Федерации.

Настоящее согласие дано мной _____ (дата) и действует в течении всего срока обработки включая все действия (операции) с моими персональными данными.

Я оставляю за собой право отозвать своё согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручён лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку моих персональных данных Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчётов по оплате оказанной мне до этого медицинской помощи.

Контактный телефон(ы) _____

и почтовый адрес _____

подпись субъекта персональных данных. _____

или законного представителя субъекта персональных данных. _____