КОМИТЕТ ЗДРАВООХРАНЕНИЯ
ВОЛГОГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

19.05.2015 № 1603

Волгоград

О введении в действие документов, регламентирующих мероприятия по защите информации ограниченного доступа, обрабатываемой в комитете здравоохранения Волгоградской области

В целях исполнения требований постановления Правительства Российской Федерации от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами" п р и к а з ы в а ю:

1. Утвердить:

1.1. Политику в отношении обработки персональных данных в комитете здравоохранения Волгоградской области (Приложение № 1).

1.2. Правила обработки и обеспечения защиты персональных данных в комитете здравоохранения Волгоградской области (Приложение № 2).

1.3. Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение № 3).

1.4. Порядок доступа в помещения, в которых ведется обработка персональных данных (Приложение № 4).

1.5. Регламент предоставления прав доступа к информации в информационных системах комитета здравоохранения Волгоградской области (Приложение № 5).

1.6. Правила работы с обезличенными данными комитета здравоохранения Волгоградской области (Приложение № 6).

1.7. Форму согласия субъекта на обработку персональных данных (Приложение № 7).

2. Специалисту 1 категории отдела демографической политики Г.В.Когуту в срок не позднее 15.05.2015 разместить документы,

определяющие политику в отношении обработки персональных данных, на официальном сайте комитета здравоохранения Волгоградской области.

3. Приказ министерства здравоохранения Волгоградской области от 03.02.2014 № 200 "О введении в действие документов, регламентирующих мероприятия по защите информации ограниченного доступа, обрабатываемой в министерстве здравоохранения Волгоградской области" признать утратившим силу.

4. Контроль исполнения настоящего приказа возложить на заместителя председателя комитета И.А.Карасеву.

Председатель комитета здравоохранения Волгоградской области  В.В.Шкарин

Р.В.Михин
(8442) 24-86-77

ПРИЛОЖЕНИЕ № 1

к приказу комитета
здравоохранения
Волгоградской области

от 19.05.2015 года № 1603

Политика
в отношении обработки персональных данных в комитете здравоохранения Волгоградской области

1. Общие положения

Настоящая Политика разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ "О персональных данных" (далее – Федеральный закон), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (далее – ПП №1119), постановлением Правительства Российской Федерации от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ними нормативными правовыми актами, операторами являющимися государственными или муниципальными органами" (далее – ПП №211) и устанавливает единый порядок обработки персональных данных в комитете здравоохранения Волгоградской области (далее - комитет).

В документе используются следующие термины и понятия:

персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

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;

информационная система персональных данных - 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;

обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо

извлеченных из такой системы, 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.

2. Основные условия проведения обработки персональных данных

Обработка персональных данных осуществляется:

после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;

после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Волгоградской области, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;

после принятия необходимых мер по защите персональных данных.

В комитете приказом руководителя назначается сотрудник, ответственный за организацию обработки персональных данных и определяется перечень лиц, допущенных к обработке персональных данных.

Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим документом (далее – политика) и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме утвержденной приказом по комитету.

Запрещается:

обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;

осуществлять ввод персональных данных под диктовку.

3. Порядок определения защищаемой информации

Комитет создает в пределах своих полномочий, установленных в соответствии с федеральными законами, информационные системы, в целях обеспечения реализации прав объектов персональных данных.

В комитете на основании "Перечня сведений конфиденциального характера", утвержденного Указом Президента Российской Федерации 06.03.1997 № 188, определяется и утверждается перечень сведений ограниченного доступа, не относящихся к государственной тайне (далее - защищаемая информация) и перечень информационных систем персональных данных.

На стадии проектирования каждой информационной системы определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых персональных данных

4. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

Обработка персональных данных в информационных системах комитета с использованием средств автоматизации осуществляется в

соответствии с требованиями ПП №1119 и ПП №211, нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

Оператором осуществляется определение уровня защищенности информационных систем в соответствии с ПП №1119 в зависимости от категории обрабатываемых данных, их количества и наличия трудовых взаимоотношений с комитетом.

Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", а также от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

утвержденных организационно-технических документов о порядке эксплуатации информационных систем, включающих акт по установлению уровня защищенности данных, инструкции пользователя, администратора, по организации антивирусной защиты, и других нормативных и методических документов;

настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с частной моделью угроз безопасности персональных данных;

охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

Комитет прекращает обработку персональных данных или обеспечивает прекращение их обработки лицом, действующим по поручению комитета, в случае:

изменения, признания утратившими силу нормативно-правовых актов, устанавливающих правовые основания обработки персональных данных;

изменения или расторжения соглашений, заключенных комитетом во исполнение нормативно-правовых актов, на основании которых осуществляется обработка персональных данных;

выявление неправомерной обработки персональных данных осуществляемой комитетом или лицом, действующим по поручению комитета;

достижение цели обработки персональных данных;

отзыва субъектом персональных данных согласия на обработку его персональных данных, если в соответствии с законодательством Российской

Федерации обработка персональных данных допускается только с согласия субъекта персональных данных.

5. Ответственность должностных лиц

Гражданские государственные служащие, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ № 2

к приказу комитета
здравоохранения
Волгоградской области

от 19.05.2015 года № 1603

Правила обработки и обеспечения защиты персональных данных в комитете здравоохранения Волгоградской области

1. Общие положения

1.1. Настоящие правила обработки и обеспечения защиты персональных данных (далее - Правила) комитета здравоохранения Волгоградской области (далее – комитет) разработаны в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных в информационных системах персональных данных.

1.2. Целью настоящего документа является формирование общих правил для обеспечения защиты комитетом персональных данных (далее - ПДн) от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн.

1.3. Правила разработаны в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом Российской Федерации от 27.07.2006 г. № 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства Российской Федерации от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" и иными нормативными актами, действующими на территории Российской Федерации. В соответствии с Указом Президента Российской Федерации от 30.05.2005 № 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела", настоящие Правила должны быть дополнены положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела.

1.4. В Правилах используются следующие термины:

Безопасность персональных данных – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в информационной системе.

Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Информационная система персональных данных – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

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 (в данном случае комитетом) или иным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Неавтоматизированная обработка персональных данных – обработка ПДн субъекта без использования средств вычислительной техники.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

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 ПДн.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

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.

Трансграничная передача персональных данных – передача ПДн на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе и (или) в результате которых уничтожаются материальные носители ПДн.

2. Область действия

2.1. Правила являются обязательными для исполнения всеми работниками комитета, имеющими доступ к персональным данным.

3. Рекомендации по защите

3.1. Рекомендации содержат описание системы мер и принципов организации защиты ПДн в комитете.

3.2. Рекомендуется устанавливать в технических заданиях на создание (модернизацию) конкретных информационных систем и элементов информационно-телекоммуникационной инфраструктуры такой уровень требований по защите информации, который бы соответствовал или был строже рекомендаций, предложенных в настоящем разделе.

3.3. Работы по защите информации проводятся на основе реализации комплекса организационных и технических мероприятий.

3.4. Не допускается осуществление работниками комитета любых мероприятий и работ с использованием ПДн без принятия необходимых мер по защите информации.

3.5. Организация работ по обработке и защите информации в комитете возлагается на работника, ответственного за организацию обработки и обеспечение безопасности ПДн, назначенного приказом председателя комитета, или на стороннюю организацию (далее – Уполномоченное лицо) по договору.

3.6. Координация работ в области защиты информации и контроль эффективности мер защиты информации возлагаются на работника комитета, ответственного за организацию обработки и обеспечение безопасности ПДн.

3.7. Методическое руководство, подготовка нормативно-распорядительной документации и реализация технических мер по обеспечений безопасности обработки персональных данных возлагаются на работника комитета, ответственного за выполнение вышеуказанных работ, или на сотрудника Уполномоченного лица при условии выполнения требований п.3.8 настоящих Правил.

3.8. Для обеспечения технической защиты ПДн могут привлекаться организации, имеющие лицензии на указанный вид деятельности, так как деятельность по технической защите конфиденциальной информации является лицензируемым видом деятельности и должна осуществляться на основе лицензий, выданных уполномоченными федеральными органами исполнительной власти.

4. Обработка персональных данных субъектов персональных данных

4.1. Все ПДн субъекта ПДн следует получать работникам комитета, допущенным к обработке ПДн, у него самого. Если ПДн субъекта возможно получить только у третьей стороны, за исключением случаев, предусмотренных законодательством Российской Федерации, субъект должен быть уведомлен об этом заранее в письменном виде по почте работником, ответственным за организацию обработки и обеспечение безопасности ПДн, или другим сотрудником комитета по его поручению. Работник комитета, принимающий ПДн субъекта, должен сообщить субъекту ПДн следующую информацию:

наименование, либо фамилия, имя, отчество и адрес комитета или его представителя;

цель обработки ПДн и ее правовое основание;

предполагаемые пользователи ПДн;

установленные действующим законодательством РФ права субъекта ПДн.

4.2. Работники комитета не имеют права получать и обрабатывать ПДн субъектов, не соответствующие целям их обработки.

4.3. Обработка специальных категорий ПДн субъектов, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, возможна только с их согласия либо без их согласия в случаях, установленных законодательством РФ.

4.4. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в письменной форме, если иное не установлено Федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн, полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются работником, ответственным за организацию обработки и обеспечение безопасности ПДн или другим сотрудником комитета по его поручению, на основе нотариально заверенных доверенностей либо других документов, подтверждающих полномочия представителей, копии которых должны быть приложены к согласию.

4.5. Передавать ПДн субъектов для обработки третьим лицам можно только после получения комитетом от субъекта ПДн письменного согласия на передачу конкретному лицу (организации), кроме случаев, установленных действующим законодательством РФ. Передача ПДн на материальном носителе информации фиксируется в соответствующих журналах сотрудниками, ответственными за документооборот в комитете. Передача ПДн в электронном виде по защищенным каналам связи фиксируется в электронных журналах средств защиты информации.

4.6. Письменное согласие субъекта ПДн на обработку его ПДн должно включать в себя:

фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты и приложенная нотариальная копия (или оригинал) доверенности или иного надлежащего документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

наименование и адрес комитета;

цель обработки ПДн;

перечень ПДн, на обработку которых дается согласие субъекта ПДн;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению комитета, если обработка будет поручена такому лицу;

перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых комитетом способов обработки ПДн;

срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено действующим законодательством РФ;

подпись субъекта ПДн.

4.7. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн или в случае достижения целей обработки ПДн, Работник, ответственный за организацию обработки и обеспечение безопасности ПДн либо сотрудник комитета по его поручению, инициирует сбор, блокировку обработки с последующим уничтожением ПДн субъекта, кроме случаев, установленных законодательством РФ.

4.8. Письменные согласия субъектов передаются Работнику, ответственному за организацию обработки и обеспечение безопасности ПДн, и хранятся в специально предназначенном месте.

4.9. При обработке ПДн субъекта, по его запросу могут быть предоставлены следующие данные:

подтверждение факта обработки ПДн в комитете;

правовые основания и цели обработки ПДн;

цели и применяемые в комитете способы обработки ПДн;

наименование и место нахождения комитета, сведения о лицах (за исключением работников комитета), которые имеют доступ к персональным данным или которым могут быть раскрыты ПДн на основании договора с комитетом или на основании Федерального закона;

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

сроки обработки ПДн, в том числе сроки их хранения;

порядок осуществления субъектом ПДн прав, предусмотренных настоящим Федеральным законом;

наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению комитета, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом Российской Федерации от 27.07.2006 г. № 152-ФЗ "О персональных данных" или другими Федеральными законами.

4.10.В случае получения запросов от уполномоченного органа по защите прав субъектов ПДн работник, ответственный за организацию обработки и обеспечение безопасности ПДн либо сотрудник комитета по его поручению, обязан представить документы и локальные акты, по обеспечению безопасности обработки ПДн субъектов и (или) иным образом подтвердить принятие необходимых мер в течение тридцати дней с даты получения такого запроса.

4.11.В соответствии с законодательством РФ в целях обеспечения прав и свобод человека и гражданина комитет и его представители при обработке ПДн субъекта должны соблюдать следующие общие требования:

обработка ПДн может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов РФ;

при определении объема и содержания, обрабатываемых ПДн комитет должно руководствоваться действующим законодательством РФ и локальными нормативными актами комитета;

при принятии решений, затрагивающих интересы субъекта, комитет не имеет права основываться на ПДн субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;

защита ПДн субъекта от неправомерного их использования или утраты обеспечивается комитетом в порядке, установленном действующим законодательством РФ;

работники комитета должны быть ознакомлены под роспись с документами комитета, устанавливающими порядок обработки ПДн, а также об их правах и обязанностях в этой области;

доступ Работников комитета к персональным данным субъектов ПДн в информационных системах регламентируется только на основании локальных нормативных актов комитета с указанием перечня допущенных лиц, прав доступа, необходимых для выполнения служебных обязанностей;

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

уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление);

уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными;

при хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

4.12.При передаче ПДн субъекта работниками комитета должны соблюдаться следующие требования:

не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных Федеральным законом;

осуществлять передачу ПДн субъектов в пределах комитета в соответствии с нормативными документами внутреннего документооборота комитета.

4.13.Допускается передача ПДн субъектов сторонним организациям, если данная передача обусловлена Федеральным законом, либо соответствующим соглашением, и не нарушает прав субъекта ПДн.

4.14.В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя или уполномоченного органа по защите прав субъектов ПДн должно быть осуществлено блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом,

действующим по поручению комитета) с момента такого обращения или получения указанного запроса на период внутренней проверки в комитете.

4.15.В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн, должно быть осуществлено блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечено их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению комитета) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

4.16.В случае подтверждения факта неточности ПДн на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, должно быть проведено уточнение ПДн работником, ответственным за организацию обработки и обеспечение безопасности ПДн, либо обеспечено их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению комитета) в течение семи рабочих дней со дня представления таких сведений и снято блокирование ПДн. Уточнение ПДн должно производиться на основании данных, полученных от субъекта ПДн.

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

4.18.В случае достижения цели обработки ПДн комитет обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению комитет) и уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению комитета) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено законодательством Российской Федерации либо договором, стороной которого, выгодоприобретателем или поручителем по которому является

субъект ПДн, иным соглашением между комитетом и субъектом ПДн, либо если комитет не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законодательством.

4.19.В случае отзыва субъектом ПДн согласия на обработку его ПДн комитет обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством Российской Федерации либо договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между комитетом и субъектом ПДн либо, если комитет не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законодательством.

4.20.В случае невозможности уничтожения ПДн в течение срока, указанного в п. 4.17 – 4.19, комитет осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению комитета) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен Федеральными законами.

4.21.Работники комитета несут персональную ответственность за сохранность ПДн, к которым они имеют доступ.

4.22.Работники комитета, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, могут быть привлечены к ответственности, предусмотренной действующим законодательством РФ и локальными нормативными актами комитета.

5. Оценка угроз безопасности информации

5.1. Информация, обрабатывающаяся в информационных системах комитета, телекоммуникационных сетях, представляет интерес для конкурентов, коммерческих организаций и криминальных структур.

5.2. Материальными носителями ПДн, применяющимися в технических средствах и системах, являются: бумажные носители, накопители на жестких магнитных дисках, оптические и магнитные диски и ленты, флэш-память.

5.3. Основные виды угроз и источники угроз безопасности представлены в модели угроз безопасности для каждой автоматизированной информационной системы комитета.

6. Организационные мероприятия по защите персональных данных при их обработке и передаче в информационных системах комитета

6.1. В общем случае организационные мероприятия по защите ПДн связаны с формированием системы документов по защите ПДн, их разработкой, официальным оформлением и доведением до исполнителей, а также организацией контроля за соблюдением установленных этими документами правил и требований.

6.2. Мероприятия должны исключить возможность утечки информации, обрабатываемой в информационных системах комитета, и обеспечить запрет передачи ПДн по открытым каналам связи без применения установленных мер по ее защите, а также исключить возможность внесения в контролируемую зону устройств регистрации и накопления информации без соответствующего разрешения.

6.3. Система документов по защите информации включает действующее законодательство РФ и локальные нормативные акты комитета.

6.4. Состав внутренних документов, разрабатываемых на основании действующего законодательства РФ и локальных нормативных актов комитета, определяется на этапе приведения процессов обработки ПДн в комитете в соответствие требованиям законодательства. Состав документов определяется комитетом при возможном привлечении организаций-лицензиатов.

6.5. В подразделении, обслуживающем информационную систему комитета, рекомендуется иметь комплект эксплуатационной и технической документации на информационную систему, в том числе на систему защиты ПДн.

6.6. Обязанность поддерживать комплект документов по защите ПДн в актуальном состоянии возлагается на работника, ответственного за организацию обработки и обеспечение безопасности ПДн.

6.7. Организационные мероприятия по защите ПДн, обрабатываемых на автоматизированных рабочих местах (далее - АРМ), должны быть связаны с обеспечением:

сохранности машинных носителей информации, материалов печати и исключения доступа к ним посторонних лиц;

ограничения физического доступа и контроль доступа к изменению конфигурации средств электронно-вычислительной техники (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.);

исключения возможностей несанкционированного просмотра изображений с монитора АРМ через дверные проемы, окна – в том числе с использованием средств телевизионной, фотографической и визуальной оптической разведки, находящихся за границами контролируемой зоны;

режима блокирования доступа к АРМ во время отсутствия работника комитета;

режима блокирования доступа в помещение с установленным АРМ во внерабочее время и в рабочее время при отсутствии работника комитета.

6.8. Организационные мероприятия по защите ПДн в локальных вычислительных сетях (далее – ЛВС) должны включать:

обеспечение режима запрета на вхождение в сеть под чужой учетной записью;

обеспечение периодической смены паролей работниками комитета;

обеспечение хранения файлов с информацией в групповых каталогах (каталогах, информация в которых является доступной для определенной группы лиц), структура которых однозначно отображает организационную структуру подразделения (управления, отдела, группы и др.) и разрешения доступа к нему только Работников соответствующей структурной единицы;

обеспечение файлового обмена информацией между работниками комитета подразделений через создаваемый каталог общего использования, информация в котором является доступной для имеющих санкционированный доступ в ЛВС работников комитета;

обеспечение создания для каждого работника комитета личного сетевого каталога, предназначенного для хранения пользовательских данных, и предоставление ему всех прав (чтение, запись, создание, удаление, переименование) в отношении информации указанного каталога, за исключением права изменения привилегий доступа;

обеспечение контроля присвоения работника комитета учетных записей и их удаление или блокирование при увольнении работника;

обеспечение резервного копирования электронных информационных ресурсов;

обеспечение режима разграничения и контроля доступа к аппаратным и программным ресурсам локальных вычислительных сетей и АРМ.

7. Технические мероприятия по защите персональных данных

7.1. Технические мероприятия по защите информации разрабатываются по результатам обследования объекта информатизации, предназначенного для обработки ПДн, и оценки возможностей реализации замысла защиты на основе применения организационных мер защиты и активизации встроенных механизмов защиты используемых операционных систем и аппаратного обеспечения. Соответствующие требования излагаются в техническом задании на проектирование системы защиты.

7.2. Требуется осуществлять следующие технические мероприятия:

применение сертифицированных программных и (или) аппаратных средств защиты информации от несанкционированного доступа, контроля целостности, регистрации и учета действий пользователей информационной системы;

применение сертифицированных средств криптографической защиты конфиденциальной информации при ее передаче по открытым каналам связи;

предотвращение несанкционированной записи ПДн на съемные носители информации или вывода ПДн на печать;

регулярный анализ защищенности системы защиты ПДн;

защита ПДн при межсетевом взаимодействии;

применение антивирусной защиты.

8. Контроль состояния системы защиты персональных данных

8.1. В рамках проверок состояния защиты ПДн рекомендуется осуществлять контроль:

наличия в подразделениях нормативных документов по защите информации и доведения их до персонала с фиксацией факта ознакомления с документами;

знания и выполнения работниками требований локальных нормативных актов комитета по защите ПДн при их обработке в информационных системах комитета;

наличия и комплектности эксплуатационной и технической документации на систему защиты ПДн, а так же факта ознакомления работников комитета с инструкциями пользователей и администраторов средств защиты информации с соответствующей отметкой об ознакомлении в инструкциях;

работоспособности системы защиты ПДн;

задания требований по безопасности ПДн при разработке (модернизации) информационных систем комитета.

8.2. Контроль состояния защиты ПДн осуществляется в плановом и внеплановом порядке ответственным за организацию обработки и обеспечение безопасности ПДн Работником (либо комиссией), назначаемым комитетом.

8.3. Результаты проверок оформляются в виде отчетов о проведении проверки.

9. Цели обработки данных в информационных системах

9.1. Цели обработки данных в информационных системах определяются в рамках каждой информационной системы отдельно в соответствующей модели угроз, утверждаемой в установленном порядке, с обязательным указанием нормативных документов, регламентирующих сроки хранения. В области здравоохранения документами, регламентирующими цели обработки и сроки обработки являются: Федеральный закон Российской Федерации от 21.11.2011 № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Федеральный закон Российской Федерации от 22.10.2004 № 125-ФЗ "Об архивном деле в Российской Федерации", Приказ Министерства здравоохранения Российской Федерации от 21.12.2012 № 1341н "Об утверждении Порядка ведения единого реестра лицензий, в том числе лицензий, выданных органами государственной власти субъектов Российской Федерации в

соответствии с переданным полномочием по лицензированию отдельных видов деятельности" и другие.

10. Сроки хранения данных в информационных системах

10.1. Для каждой цели обработки данных определяется срок хранения и порядок уничтожения данных либо материальных носителей информации.

10.2. Сроки хранения отдельных документов

Вид документа	Срок хранения
Сведения, справки о совокупном доходе работников за год и уплате налогов	5 лет
Документы о начисленных и перечисленных суммах налогов, об освобождении от них, о предоставленных льготах, отсрочках по уплате налогов	
Лицевые счета работников	75 лет
Личные дела:	
— руководителя организации, членов руководящих, исполнительных, контрольных органов организации, а также работников, имеющих государственные и иные звания, премии, награды, ученые степени	Постоянно
— остальных работников	75 лет
Трудовые договоры, трудовые соглашения, не вошедшие в состав личных дел, личные карточки работников (включая временных)	
Документы лиц, не принятых на работу	1 год
Перечень лиц, имеющих право подписи первичных документов	До замены новыми
Положения, инструкции о правах и обязанностях должностных лиц (должностные инструкции) типовые	Постоянно
Положения, инструкции о правах и обязанностях должностных лиц (должностные инструкции) индивидуальные	75 лет
Коллективные договоры	Не менее 10 лет (присланные для сведения - до минования надобности)
Табели (графики), журналы учета рабочего времени	5 лет (при тяжелых и опасных условиях труда - 75 лет)
Документы о премировании	5 лет
Штатные расписания и изменения к ним: а) по месту	Не менее 10 лет 3

разработки и/или утверждения; б) в других организациях	года
Личные карточки работников (в том числе временных)	75 лет
Подлинные личные документы (трудовые книжки, дипломы, аттестаты, удостоверения, свидетельства)	До востребования (невостребованные - 75 лет)
Командировочные удостоверения	5 лет после возвращения из командировки
Документы (служебные задания, отчеты, переписка) о командировании работников	5 лет
Документы (отчеты, акты, сведения) об учете трудовых книжек и вкладышей к ним	3 года
Графики предоставления отпусков	1 год
Медицинская карта стационарного больного	25 лет
Медицинская карта прерывания беременности	5 лет
История родов	25 лет
История развития новорожденного	25 лет
Протокол на случай выявления у больного запущенной формы злокачественного новообразования	5 лет
Выписка из медицинской карты стационарного больного злокачественным новообразованием	10 лет
Лист основных показателей состояния больного, находившегося в отделении (палате) реанимации и интенсивной терапии	25 лет
Лист основных показателей состояния больного, находившегося в отделении (палате) реанимации и интенсивной терапии кардиологического отделения	25 лет
Протокол (карта) патологоанатомического исследования	10 лет
Направление на патолого-гистологическое исследование	1 год
Акт констатации биологической смерти	25 лет
Статистическая карта выбывшего из стационара	10 лет
Статистическая карта выбывшего из психиатрического (наркологического) стационара	50 лет

10.3. Если в процессе работы сотрудников комитета выявляется необходимость обработки данных (материальных носителей, содержащих

информацию), не включенных в вышеуказанный перечень, необходимо провести уточнение сроков хранения и внести необходимые изменения в п.10.2 настоящих Правил.

11. План контрольных мероприятий

11.1. С целью выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, ответственными лицами проводятся контролирующие мероприятия.

Наименование контрольного мероприятия, проводимого в комитете	Периодичность проведения	Исполнитель
Контроль над соблюдением режима обработки ПДн	Ежемесячно	Системный администратор
Контроль над соблюдением режима защиты ПДн	Ежедневно	Руководитель подразделения
Контроль над выполнением антивирусной защиты	Еженедельно	Системный администратор
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Системный администратор
Проведение контрольных проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	Системный администратор
Контроль обновления программного обеспечения	Еженедельно	Системный администратор
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных угроз	Ежегодно	Системный администратор
Поддержание в актуальном состоянии нормативно-организационных документов	Ежеквартально	Системный администратор
Контроль выполнения работниками Учреждения инструкций по защите ПДн.	Еженедельно	Руководитель подразделения
Контроль знания и выполнения Работников требований локальных нормативных актов комитета по защите ПДн в АРМ и ЛВС путем выборочного опроса работников.	Ежеквартально	Системный администратор

11.2. При возникновении внештатных ситуаций, повлекших несанкционированное уничтожение данных, нарушение целостности и другие несанкционированные изменения информации, проводятся внеплановые контролирующие мероприятия в структурном подразделении комитета, в котором возникла внештатная ситуация.

ПРИЛОЖЕНИЕ № 3

к приказу комитета
здравоохранения
Волгоградской области

от 19.05.2015 года № 1603

Правила рассмотрения запросов субъектов персональных данных или их представителей

1. Общие положения

1.1. Правила рассмотрения на запросы субъектов персональных данных (далее - Правила) разработаны в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - ФЗ № 152-ФЗ) и определяют порядок обработки обращений субъектов персональных данных с запросами о предоставлении комитетом здравоохранения Волгоградской области (далее - комитет или оператор) персональных данных (далее - ПДн), имеющихся в информационных системах обработки персональных данных.

1.2. Настоящие правила определяют порядок получения работниками комитета (далее - Работник/-ки) запросов субъектов ПДн, дальнейшие действия Работников при получении запросов субъектов ПДн, порядок обработки запросов ответственными в этой компетенции Работниками, порядок формирования ответов на запросы, а также порядок передачи ответов на запросы субъектам ПДн.

2. Порядок обращения субъекта ПДн к оператору, действия ответственного Работника оператора, принявшего запрос

2.1. Субъект ПДн имеет право обратиться к оператору с письменным запросом на получение следующих сведений, за исключением случаев, предусмотренных действующим законодательством Российской Федерации (далее - РФ):

подтверждение факта обработки ПДн оператором;

правовые основания и цели обработки ПДн;

цели и применяемые оператором способы обработки ПДн;

наименование и место нахождения оператора, сведения о лицах (за исключением Работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании действующего законодательства РФ;

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен действующим законодательством РФ;

сроки обработки ПДн, в том числе сроки их хранения;

порядок осуществления субъектом ПДн прав, предусмотренных действующим законодательством РФ;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные действующим законодательством РФ.

2.2. Обращение может поступить как в письменном, так и в устном виде к оператору.

2.3. Запрос субъекта ПДн на предоставление информации, отраженной в п. 2.1 Правил, должен содержать следующую обязательную информацию:

номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя;

реквизиты доверенности законного представителя субъекта ПДн или иного документа, предусмотренного действующим законодательством РФ, на основании которого действует законный представитель;

сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки Пдн оператором.

2.4. При предъявлении письменного запроса субъект ПДн обязан предъявить основной документ, удостоверяющий личность субъекта ПДн, а законный представитель субъекта ПДн должен предъявить оригинал нотариально заверенной доверенности от субъекта ПДн (или иной документ, предусмотренный действующим законодательством РФ) с указанием полномочий, в том числе получение сведений от оператора и предоставить оператору заверенную копию вместе с запросом.

2.5. В случае устного обращения субъекта персональных данных с требованием предоставить информацию о наличии персональных данных Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, обязан предоставить субъекту персональных данных бланк запроса, форма которого должна быть утверждена комитетом в установленном порядке. Учитывая тот факт, что в запросе содержится конфиденциальная информация субъекта, Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, обязан предоставить субъекту конверт для помещения запроса.

2.6. В случае получения запроса от субъекта ПДн почтовым отправлением Работник, получивший запрос, обязан направить его в адрес Работника, ответственного за организацию обработки и обеспечение безопасности ПДн либо уполномоченного им сотрудника.

2.7. Все обращения субъектов персональных данных должны быть переданы Работнику, ответственному за организацию обработки и

обеспечение безопасности ПДн либо уполномоченного им сотрудника, в течение 1 (одного) рабочего дня от даты получения запроса. Одновременно с запросом направляется пояснительная записка в свободной форме, кто из Работников, когда и при каких обстоятельствах получил на руки запрос субъекта.

2.8. В случае получения запроса в электронной форме и подписанный электронной подписью в соответствии с требованиями федеральных законов РФ, также инициализируется процедура ответа субъекту в порядке, предусмотренном Правилами.

2.9. Сведения по запросам субъектов должны быть предоставлены субъекту ПДн в доступной форме и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

2.10. В случае, если сведения, указанные в п.2.1 Правил, а также обрабатываемые ПДн, были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно или направить повторный запрос в целях получения сведений, указанных в п.2.1 Правил и ознакомления с такими ПДн не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законодательством РФ, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

2.11. Субъект ПДн вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в п.2.1 Правил, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 2.10 Правил, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п.2.1 Правил, должен содержать обоснование направления повторного запроса.

2.12. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным п. 2.10, 2.11 Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

3. Порядок регистрации запроса субъекта ПДн

3.1. Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, в день получения запроса обязан зарегистрировать принятый запрос.

3.2. Все запросы и ответы на них должны храниться в помещении комитета, защищенном от несанкционированного доступа третьих лиц.

4. Проверка наличия/отсутствия персональных данных субъекта персональных данных в информационных системах оператора

4.1. По факту регистрации запроса Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, либо уполномоченное им лицо внимательно изучает запрос на предмет соответствия требованиям действующего законодательства РФ. Если возникают сомнения в правильности оформления запроса, то он обязан получить консультацию Работника отдела правового обеспечения комитета.

4.2. В случае, если запрос оформлен ненадлежащим образом, а именно: в нем отсутствует информация о субъекте ПДн, подпись субъекта или его законного представителя или иная информация, которая должна быть отражена в соответствии с формой запроса на предоставление сведений, утвержденной комитетом, то Работник, ответственный за организацию обработки и обеспечение безопасности ПДн либо уполномоченное им лицо оформляет отказ в предоставлении информации.

4.3. В случае, если запрос оформлен в соответствии с требованиями законодательства РФ, то Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, либо уполномоченное им лицо с привлечением пользователями информационной системы, в которой обрабатывается искомая информация, находит всю информацию о субъекте ПДн и распечатывает отчет по персональным данным субъекта из информационной системы оператора, или констатирует факт, что ПДн о субъекте в информационной системе отсутствуют. В зависимости от результатов поиска ПДн субъекта ПДн Работник, ответственный за обработку запросов, составляет ответ на запрос субъекта ПДн.

4.4. Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, либо уполномоченное им лицо в целях скорейшего сбора информации может направить запрос о субъекте пользователям информационных систем комитета по электронной почте, поставив в копию непосредственного руководителя отдела или сектора комитета. Пользователи информационных систем комитета должны в течение 5 суток отреагировать на запрос ответственного Работника за обработку запросов и предоставить всю информацию по субъекту ПДн, а если она отсутствует, сообщить об этом.

5. Оформление и содержание ответа на запрос при наличии или отсутствии персональных данных субъекта в информационных системах оператора

5.1. В случае если в информационных системах оператора имеется или отсутствует информация о ПДн субъекта, обратившегося с запросом,

Работник, ответственный за обработку запроса, составляет ответ на запрос субъекта в произвольной форме по существу вопросов.

5.2. Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, либо уполномоченное им лицо:

подписывает ответ на запрос с приложением отчета по персональным данным субъекта, ставит печать комитета, делает копию отчета из информационной системы, формирует опись документов и один экземпляр описи с подготовленными документами упаковывает в конверт для отправки посредством почтового отправления с уведомлением о вручении, либо готовит ответ с описанными в настоящем пункте документами для вручения субъекту ПДн или его законному представителю способом, указанным в запросе, под подпись;

дубликат ответа с иными перечисленными в описи документами, а также с оригиналом описи, отправленной почтовым отправлением или врученной субъекту ПДн или его законному представителю под подпись, прикладываются к запросу и хранятся вместе с запросом;

в журнале учета обращений субъектов персональных данных по выполнению их законных прав делает отметку об ответе на запрос, краткое содержание ответа (положительный, отрицательный, отказ), отражает дату отправления ответа, способ его отправления (почтовое отправление, отправление на объект комитета для передачи субъекту через ответственного Работника комитета, лично в руки субъекту или его законному представителю), а также ставит свою подпись в разделе "подпись работника, ответственного за обработку запроса" журнала регистрации запросов.

5.3. При почтовом отправлении конверт с подготовленными ответом и приложенными документами запечатывается в почтовом отделении в присутствии Работника почтового отделения. В конверт вкладывается один экземпляр почтовой описи со штампом почтового отделения. При почтовом отправлении конверт с ответом, приложенными документами и описью отправляется субъекту ПДн с уведомлением о вручении.

5.4. Если субъект ПДн выразит желание получить лично на руки ответ или через своего законного представителя, Работник, ответственный за организацию обработки и обеспечение безопасности ПДн, передает лично подготовленные документы под подпись. Дубликат ответа с оригинальной подписью субъекта ПДн или его законного представителя после должен быть передан незамедлительно Работнику, ответственному за организацию обработки и обеспечение безопасности ПДн, для хранения.

5.5. Срок ответа на запрос субъекта персональных данных не может превышать 30 (тридцати) календарных дней от даты получения запроса от субъекта, если иной срок не будет установлен действующим законодательством РФ.

ПРИЛОЖЕНИЕ № 4

к приказу комитета
здравоохранения
Волгоградской области

от 19.05.2015 года № 1603

Порядок доступа в помещения, в которых ведется обработка персональных данных

1. Общие положения

1.1. Порядок доступа в помещения, в которых ведется обработка персональных данных, к техническим средствам защиты информации, а также в помещения и сооружения, в которых они установлены (далее - Порядок) определяет технические меры по обеспечению контроля и управления физическим доступом в комитете здравоохранения Волгоградской области (далее – комитет).

1.2. Настоящий Порядок определяет ответственных лиц за контроль и управление физическим доступом к техническим средствам защиты информации, а также в помещения и сооружения, в которых они установлены в комитете.

2. Обеспечение контроля и управления физическим доступом к техническим средствам защиты информации

2.1. Контроль и управление физическим доступом в комитет осуществляется контрольно-пропускной службой, которую должен обеспечить собственник здания.

2.2. Выявление фактов несанкционированного доступа в контролируемую зону комитета осуществляется с помощью камер наблюдения, установленных службой охраны собственников здания, в котором располагается комитет.

3. Ответственные за организацию контроля и управления физическим доступом к техническим средствам защиты информации

3.1. Ответственность за повседневный контроль возлагается на руководителей подразделений комитета.

3.2. Ответственность за периодический контроль возлагается на системного администратора.

3.3. Ответственность за управление физическим доступом в помещения обработки информации и доступа к техническим средствам защиты информации в комитете возлагается на руководителей подразделений комитета.

3.4. В случае приема и сдачи помещений комитета под охрану данный факт должен фиксироваться в соответствующем журнале.

ПРИЛОЖЕНИЕ № 5

к приказу комитета
здравоохранения
Волгоградской области

от 19.05.2015 года № 1603

Регламент предоставления прав доступа к информации в информационных системах комитета здравоохранения Волгоградской области

1. Общие положения

1.1. Регламент предоставления прав доступа к информации в информационных системах комитета здравоохранения Волгоградской области (далее – регламент) является локальным нормативным актом комитета здравоохранения Волгоградской области (далее – комитет).

1.2. Разграничение прав осуществляется на основании выполнения должностных полномочий работниками комитета (далее – Работники или Пользователи), а также исходя из характера и режима обработки персональных данных (далее – ПДн) в информационных комитета.

1.3. Регламент определяет операции по внесению изменений в списки Пользователей и наделению их полномочиями доступа к ресурсам информационных систем, устанавливает порядок изменения списка Пользователей и порядок изменения их прав при пользовании информационными системами.

1.4. Работники, задействованные в обеспечении функционирования информационных систем, знакомятся с основными положениями и приложениями регламента в части, касающейся их, и по мере необходимости.

1.5. Ознакомление с положениями регламента Пользователей информационных систем осуществляет Работник, ответственный за организацию обработки и обеспечение безопасности ПДн либо уполномоченное им лицо, под роспись с выдачей электронных копий (при необходимости) соответствующих приложений и разделов регламента непосредственно для повседневного использования в работе.

2. Порядок использования учетных записей Пользователей

2.1. С целью соблюдения принципа персональной ответственности за свои действия каждому Работнику комитета, допущенному к работе в информационных системах комитета, должно быть предоставлено персональное уникальное имя (далее – учетная запись), под которым он будет регистрироваться и работать в системе, содержащей ПДн либо другую информацию ограниченного доступа.

2.2. В случае производственной необходимости некоторым Работникам могут быть предоставлены несколько учетных записей.

2.3. Использование несколькими Работниками при самостоятельной работе в информационных системах комитета одной и той же учетной записи Пользователя ("группового имени") запрещено.

3. Порядок предоставления Пользователям прав доступа к информационным системам комитета

3.1. Процедура регистрации (создания учетной записи) Пользователя и предоставления (изменения) ему прав доступа к ресурсам информационных систем осуществляется на основании заявки, оформляемой непосредственным руководителем Работника после чего системным администратором создается учетная запись для соответствующего Пользователя.

3.2. При предоставлении Работнику прав доступа к информационным системам необходимо руководствоваться принципом предоставления минимально необходимых прав для решения требуемых задач.

3.3. Руководители структурных подразделений комитета несут ответственность за минимальную достаточность прав доступа имеющихся у Пользователей их структурных подразделений. В случае наличия у Пользователей избыточных прав доступа для работы руководители структурных подразделений ставят об этом в известность Работника, ответственного за организацию обработки и обеспечение безопасности ПДн либо уполномоченное им лицо, который вносит необходимые изменения в соответствии с настоящем регламентом.

3.4. При выдаче Пользователю персонального аппаратного идентификатора (токен, смарт-карта, touch memory и т.п.), факт выдачи должен фиксироваться в журнале учета защищаемых носителей информации.

3.5. Целесообразно документирование прав доступа в электронном виде, для чего создается специальная база данных, в которой указываются следующие данные:

фамилия, имя и отчество Пользователя;

структурное подразделение;

учетная запись Пользователя;

информационная система, к которой предоставляется доступ;

права доступа;

отметка об удалении учетной записи при увольнении или переводе на другую должность и/или ином кадровом перемещении или оформлении изменений в трудовой договор с таким Работником.

3.6. Изменения в конфигурации механизмов защиты информации производятся системным администратором по согласованию с организацией, имеющей лицензию на выполнении соответствующих работ, и только в соответствии с документацией на средства защиты информации, используемой в информационных системах.

4. Ответственные за организацию и контроль выполнения инструкции

4.1. Ответственность за соблюдение требований настоящего регламента возлагается на всех Работников комитета.

4.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам управлении правами Пользователей и общий контроль состояния информационной безопасности возлагается на Работника, ответственного за организацию обработки и обеспечение безопасности ПДн либо уполномоченное им лицо.

ПРИЛОЖЕНИЕ № 6

к приказу комитета
здравоохранения
Волгоградской области

от 19.05.2015 года № 1603

Правила работы с обезличенными данными комитета здравоохранения Волгоградской области

1. Общие положения

1.1. Настоящие правила работы с обезличенными данными комитета здравоохранения Волгоградской области (далее - Правила) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и постановления Правительства Российской Федерации от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

1.2. Настоящие Правила определяют порядок работы с обезличенными данными комитета здравоохранения Волгоградской области.

1.3. Настоящие Правила утверждаются приказом председателя комитета здравоохранения Волгоградской области и действуют постоянно.

2. Термины и определения

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных":

персональные данные – 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;

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

3. Условия обезличивания

3.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае

утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

обобщение некоторых сведений;

понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город)

деление сведений на части и обработка в разных информационных системах;

другие способы.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. Для обезличивания персональных данных годятся любые способы, явно не запрещенные законодательно.

3.5. Ответственными за проведение мероприятий по обезличиванию обрабатываемых персональных данных в комитете здравоохранения являются руководители подразделений комитета.

4. Порядок работы с обезличенными персональными данными

4.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

4.2. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

4.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

правил создания и использования паролей пользователей;

правил применения антивирусных средств;

правил работы со съемными носителями (если они используется);

правил резервного копирования;

порядка доступа в помещения, где расположены элементы информационных систем.

4.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

4.5. При необходимости обезличивания должностное лицо, ответственное за обезличивание данных, методами, указанными в п.3.2. настоящего документа, проводит обезличивание персональных данных.

4.6. После обезличивания данные передаются исполнителям и обрабатываются специалистами в режиме, принятом для документов.

4.7. После обработки специалистами обезличенных данных результат обработки передается должностному лицу, ответственному за подготовку ответа, в виде отчета, либо аналитической записки, либо информационного письма, с обязательным приложением исходных обезличенных данных.

4.8. Должностное лицо, исходя из состава, цели запроса и наличии в его распоряжении методов кодирования (шифрования) информации, принимает решение о подготовке ответа с указанием первоначальных персональных данных, либо без указания последних.

ПРИЛОЖЕНИЕ № 7

к приказу комитета здравоохранения

Волгоградской области

от 19.05.2015 года № 1603

Форма согласия субъекта на обработку персональных данных

Я (далее - Субъект), _____,
(фамилия, имя, отчество)

документ удостоверяющий личность_____ № _____,
(вид документа)

выдан_____,
(кем и когда)

зарегистрированный (ая) по адресу: ____
_____,

даю свое согласие комитету здравоохранения Волгоградской области (далее - Оператор), зарегистрированному по адресу: 400001 г. Волгоград, улица Рабоче-Крестьянская 16, на обработку своих персональных данных, на следующих условиях:

1. Оператор осуществляет обработку персональных данных Субъекта исключительно в целях обработки, регистрации сведений, необходимых для оказания услуг в области оказания медицинской помощи населению на территории Волгоградской области, персональных данных работников комитета здравоохранения Волгоградской области, сведений об их профессиональной служебной деятельности.

2. Перечень персональных данных, передаваемых Оператору на обработку:

_____
_____
_____
_____
_____

3. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий: обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных), при этом общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон), а также на передачу такой

информации третьим лицам, в случаях, установленных нормативными документами вышестоящих органов и законодательством.

4. Настоящее согласие действует бессрочно.

5. Настоящее согласие может быть отозвано Субъектом в любой момент по соглашению сторон. В случае неправомерного использования предоставленных данных соглашение отзывается письменным заявлением субъекта персональных данных.

6. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п. 1 ст. 14 Закона).

"____"_____ 201__ г. _____

Подпись ФИО

Подтверждаю, что ознакомлен (а) с положениями Закона, права и обязанности в области защиты персональных данных мне разъяснены.

"___"_____ 201__ г._____ _____

Подпись ФИО