Положение
об обработке персональных данных
в ГБУЗ «ГПТД»

1. Общие положения.

1.1. Данное Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 30.12.2001г. №197-ФЗ «Трудовой кодекс РФ», Федеральными законами от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 г. № 152-ФЗ «О персональных данных», Положением «О порядке организации и проведения работ по защите конфиденциальной информации в Кувандыкском филиале ГБУЗ «ГПТД»» в целях обеспечения безопасности персональных данных сотрудников.

1.2. Положение определяет порядок обработки в ГБУЗ «ГПТД» персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

2. Термины и определения.

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

2.3. Обработка персональных – 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;

2.4. автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

2.5. распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.6. предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному кругу лиц;
2.7. блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
2.8. уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
2.9. обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
2.10. информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
2.11. трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Порядок обработки персональных данных

3.1. Цели и задачи обработки персональных данных сотрудников.

Обработка персональных данных ведется в соответствии с Федеральным законом от 30.12.2001г. № 197-ФЗ «Трудовой кодекс РФ», Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных» ст.6 ч.1 п.2, Федеральным законом от 21.11.1996г. №129 «О бухгалтерском учете», Федеральным законом от 31.07.1998г. №146-ФЗ «Налоговый кодекс РФ» часть первая.

Обработка персональных данных сотрудников ведется с целью установления гарантий трудовых прав и свобод граждан, создание благоприятных условий труда, защиты прав и интересов сотрудников и работодателей.

Основными задачами обработки персональных данных являются создание необходимых правовых условий для достижения оптимального согласования интересов сторон трудовых отношений, интересов государства, а также правовое регулирование трудовых отношений и иных непосредственно связанных с ними отношений по:

- организации труда и управлению трудом;
- трудоустройству у данного работодателя;
- профессиональной подготовке, переподготовке и повышению квалификации сотрудников ГБУЗ «ГПТД»;

- участию сотрудников в установлении условий труда и применении трудового законодательства в предусмотренных законом случаях;
- материальной ответственности работодателей и сотрудников;
- разрешению трудовых споров;
- регулирование отношений по установлению, введению и взиманию налогов и сборов;
- обеспечению информацией об использовании материальных, трудовых и финансовых ресурсов в соответствии с утвержденными нормами, нормативами и сметами;
- обязательному социальному страхованию в случаях, предусмотренных федеральными законами.

3.2. Условия обработки персональных данных сотрудников.

Обработка персональных данных ведется на основании заключаемого с этим лицом трудового договора с обязательным соблюдением конфиденциальности полученных персональных данных. Обработка персональных данных сотрудников осуществляется в соответствии со ст.6 ч.1 п.2 Федерального закона от 27.07.2006г .№152-ФЗ «О персональных данных».

ГБУЗ «ГПТД» получает персональные данные сотрудников у них самих. Персональные данные сотрудника могут быть получены от лица, не являющегося субъектом персональных данных, при условии предоставления подтверждения наличия оснований, указанных в пунктах 2-11 ч. 1 ст.6, ч.2 ст.10 и ч.2 ст.11 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных».

Сотрудник имеет право на получение информации, касающейся обработки его персональных данных, указанной в ст.14 ч.7 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных» на основании запроса, составленному в соответствии со ст.14 ч.3 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных».

Если предоставление персональных данных является обязательным в соответствии с Федеральным законом, ГБУЗ «ГПТД» обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Если персональные данные получены не от субъекта персональных данных, ГБУЗ «ГПТД», за исключением случаев, предусмотренных ст.18 ч.3 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных», до начала обработки таких персональных данных обязан предоставить сотруднику следующую информацию:

1. наименование и адрес оператора или его представителя.
2. цель обработки персональных данных и ее правовое основание.
3. предполагаемые пользователи персональных данных.

4. установленные Федеральным законом права субъекта персональных данных.
5. источник получения персональных данных.

Персональные данные хранятся:

- в электронном виде (на серверах, персональных компьютерах, а также на сменных магнитных, оптических и других цифровых носителях);
- на бумажных носителях, в том числе в личных делах сотрудников, специально оборудованных шкафах и сейфах, обеспечивающих защиту от несанкционированного доступа.

При передаче персональных данных сотрудника необходимо соблюдать следующие требования:

- не сообщать персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами.
- не сообщать персональные данные сотрудника в коммерческих целях без его письменного согласия.
- предупредить лиц, получающих персональные данные сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные сотрудника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными сотрудников в порядке, установленном Трудовым кодексом и иными федеральными законами.
- осуществлять передачу персональных данных сотрудника в пределах организации в соответствии с настоящим Положением, с которым сотрудник должен быть ознакомлен под роспись.
- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.
- не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции.
- передавать персональные данные сотрудника представителям сотрудников в порядке, установленном Трудовым кодексом и иными Федеральными законами, и ограничивать эту информацию только теми персональными данными сотрудника, которые необходимы для выполнения указанными представителями их функций.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Цели и задачи обработки персональных данных граждан.

3.3.1. Цели и задачи обработки персональных данных.

Обработка персональных данных граждан ведется в соответствии с Федеральным законом Российской федерации от 21.11.2011г. №323-ФЗ «Об основах охраны здоровья граждан в РФ», Постановление Правительства Оренбургской области от 03.11.2011г .№1075-П «О региональном фрагменте единой информационной системы в сфере здравоохранения» и Распоряжения Министерства здравоохранения от 28.10.2011г. №1279 «О региональном фрагменте единой информационной системы в сфере здравоохранения» с целью регулирования отношений, возникающих в сфере охраны здоровья граждан в РФ.

Основной задачей обработки персональных данных граждан является оказание медицинских услуг.

3.3.2. Условия обработки персональных граждан.

ГБУЗ «ГПТД» получает персональные данные граждан у них самих. Персональные данные гражданина могут быть получены Кувандыкским филиалом ГБУЗ «ГПТД» от лица, не являющегося субъектом персональных данных, при условии предоставления подтверждения наличия оснований, указанных в пунктах 2-11 ч.1 ст.6, ч.2 ст.10 и ч.2ст.11 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных».

Гражданин имеет право на получение информации, касающейся обработки его персональных данных, указанной в ст.14 ч.7 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных» на основании запроса, составленному в соответствии со ст.14 ч.3 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных».

Если предоставление персональных данных является обязательным в соответствии с ФЗ, ГБУЗ «ГПТД» обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

Если персональные данные получены не от субъекта персональных данных, ГБУЗ «ГПТД», за исключением случаев, предусмотренных ст.18 ч.4 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных», до начала обработки таких персональных данных обязан предоставить гражданину следующую информацию:

1. Наименование либо фамилия, имя, отчество и адрес оператора или его представителя.
2. Цель обработки персональных данных и ее правовое основание.
3. Предполагаемые пользователи персональных данных.
4. Установленные Федеральным законом права субъекта персональных данных.
5. Источник получения персональных данных.

Персональные данные гражданина хранятся:

- в электронном виде (на серверах, персональных компьютерах, а также сменных магнитных, оптических и других цифровых носителях)
- на бумажных носителях в специально оборудованных шкафах и сейфах, обеспечивающих защиту от несанкционированного доступа.

Персональные данные гражданина не передаются сторонним организациям, если иное не предусмотрено Федеральным законом.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.4. Ведение личных дел сотрудников ГБУЗ «ГПТД».

3.4.1. Персональные данные и иные сведения, связанные с приемом на работу, трудовой деятельностью и увольнением, вносятся в личное дело сотрудника ГБУЗ «ГПТД», в связи с трудовыми отношениями. Личные дела сотрудников ведутся отделом кадров ГБУЗ «ГПТД».

3.4.2. Совокупность персональных данных, внесенных в личные дела сотрудников, и иные сведения, содержащиеся в личных делах сотрудников, относятся к сведениям конфиденциального характера. На личное дело сотрудника ставится гриф «Для служебного пользования», на документы, хранящиеся в личном деле, гриф не проставляется.

3.4.3. К личному делу сотрудников приобщаются:

- письменное заявление о приеме на работу
- собственноручно заполненный и подписанный сотрудником личный листок по учету кадров установленной формы с приложением фотографии
- копия паспорта
- копия трудовой книжки
- копия свидетельства о государственной регистрации актов гражданского состояния
- копия документов о профессиональном образовании, персональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания
- копии решения о награждении государственными наградами, присвоении почетных, воинских и специальных званий, присуждении государственных премий
- копия приказа о приеме на работу
- экземпляр трудового договора, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор
- копии приказов о переводе сотрудника на другую постоянную работу, о переводе на другую работу временно
- копии приказов о расторжении трудового договора
- аттестационный лист сотрудника, прошедшего аттестацию
- копии документов о присвоении сотруднику квалификационного разряда
- копии приказов о поощрении сотрудника, а также о применении к нему дисциплинарного взыскания до его снятия или отмены

- документы, связанные с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности связано с использованием таких сведений
- копия страхового свидетельства обязательного пенсионного страхования

3.4.4. В личное дело сотрудника вносятся также письменные объяснения сотрудника, если такие объяснения даны им после ознакомления с документами своего личного дела.

3.4.5. Документы, приобщенные к личному делу сотрудника, брошюруются, страницы нумеруются, к личному делу прилагается опись.

3.4.6. В обязанности сотрудника, осуществляющего ведение личных дел сотрудников, входит:

3.4.6.1. формирование и обеспечение сохранности личных дел сотрудников

3.4.6.2. обеспечение конфиденциальности сведений, содержащихся в личных делах сотрудников, в соответствии с законодательством РФ и внутренними документами ГБУЗ «ГПТД».

3.4.6.3. ознакомление сотрудника с документами своего личного дела во всех случаях, предусмотренных законодательством РФ.

3.4.7. Личные дела уволенных сотрудников хранятся в отделе кадров ГБУЗ «ГПТД» в течение двух лет со дня увольнения, после чего передаются в архив.

3.5. Обязанности по уточнению, блокированию и уничтожению персональных данных.

3.5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных необходимо осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения.

3.5.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных необходимо осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.5.3. В случае подтверждения факта неточности персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых

документов уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.5.4. В случае достижения цели обработки персональных данных необходимо прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных.

3.5.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных необходимо прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных.

3.6. Права сотрудников ГБУЗ «КПТД» и граждан.

Сотрудники и граждане имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ ил иного федерального закона;
- дополнение своих персональных данных оценочного характера заявлением, выражающим собственную точку зрения;
- требование об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия при обработке и защите его персональных данных.

3.7. Организация доступа к персональным данным.

Система доступа представляет собой совокупность норм и правил, определяющих, кто из руководителей организации, кому из граждан и с какими категориями документов может давать разрешение на ознакомление.

Система доступа должна отвечать следующим требованиям:

- доступ к конфиденциальным документам может предоставляться сотрудникам, письменно оформившим с организацией отношения о неразглашении ставших им известным конфиденциальных сведений. Письменное оформление отношений о неразглашении конфиденциальной информации (соблюдения режима конфиденциальности) является обязательным условием для доступа исполнителей к документам;
- доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного исполнителя;

- система доступа должна давать возможность обеспечивать исполнителей всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;

- доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами только входящими в сферу его деятельности и только установленному кругу лиц;

- доступ должен оформляться письменно по каждому конкретному конфиденциальному документу. При необходимости ознакомления исполнителя только с частью документа в разрешении на ознакомление должны быть указаны разделы (пункты или страницы), с которыми можно ознакомить исполнителя.

Доступ сотрудников организации к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу или уже в ходе трудовых отношений. При этом необходимо выполнить следующие условия:

- ознакомить сотрудника под роспись с перечнем конфиденциальной информации;

- ознакомить сотрудника под роспись с установленным в организации режимом по охране конфиденциальности и с мерами ответственности за его нарушение;

- создать сотруднику необходимые условия для соблюдения им установленного режима по охране конфиденциальности.

Доступ к персональным данным разрешается только лицам, определенным в порядке, установленным настоящим Положением. При этом указанные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций, и в целях, для которых они сообщены.

Со стороны сотрудника предполагается принятие следующих обязательств:

- по соблюдению установленного в организации режима по охране конфиденциальности;

- о неразглашении конфиденциальной информации, ставшей ему известной в период выполнения трудовых отношений, после прекращения

трудового договора в течение срока, предусмотренного в специальном соглашении или в течение трех лет, если такое соглашение не заключалось, и не использовании этой информации в личных целях;

- о возмещении причиненного ущерба, если сотрудник виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе прекращения трудового договора);

- о возврате при прекращении или расторжении трудового договора всех имеющихся у сотрудника материальных носителей конфиденциальной информации.

Главный врач ГБУЗ «ГПТД»:

- несет ответственность за организацию защиты персональных данных в организации;

- закрепляет за сотрудниками, допущенными к обработке персональных данных, конкретные массивы носителей с персональными данными, которые необходимы для выполнения возложенных на них функций;

- осуществляет внутренний контроль за соблюдением сотрудниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных;

- доводит до сведения сотрудников положения законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

С сотрудником, допущенным к персональным данным, заключается соглашение о допуске к конфиденциальной информации в установленном порядке. Соглашение от имени ГБУЗ «ГПТД» подписывает главный врач.

Сведения о работающем (работавшем) сотруднике могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии согласия сотрудника на предоставление данных.

3.8. Обязанности лиц, допущенных к обработке персональных данных сотрудника

Лица, допущенные к работе с персональными данными, обязаны:

- знать законодательство РФ и нормативные документы ГБУЗ «ГПТД» в части обеспечения безопасности персональных данных;

- обеспечивать сохранность закрепленного массива носителей с персональными данными, исключать возможность ознакомления с ними других лиц;

- докладывать своему непосредственному руководителю обо всех фактах и попытках несанкционированного доступа к персональным данным и другим нарушениях;

- Ознакомиться под роспись с настоящим Положением, а также об их правах, обязанностях, ответственности в области защиты персональных данных.

3.9. Меры по обеспечению безопасности персональных данных в ГБУЗ «ГПТД»

В ГБУЗ «ГПТД» должны быть приняты необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных в соответствии со статьей 19 ФЗ от 27.07.2006г. №152-ФЗ «О персональных данных».

3.9.1. Организационные и технические методы защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

- Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных»
- Действующими нормативными документами ФСТЭК России:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
2. Методика определения актуальности угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
3. Приказ от 13.02.2008г. №55 об утверждении порядка проведения классификации информационных систем персональных данных.
4. Приказ от 05.02.2010г. №58 об утверждении положения о методах и способах защиты информации в информационных системах персональных данных.

- Действующими нормативными документами ФСБ России:

1. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.
2. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.
3. Типовой регламент проведения в пределах полномочий и мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

- Действующими документами Роскомнадзора:
- Приказ от 17.07.2008г. №08 «Об утверждении образца формы уведомления об обработке персональных данных»;
- Приказ от 01.12.2009г. №630 «Об утверждении административного регламента проведения проверок федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных;
- Приказ от 30.01.2010г. №18 «Об утверждении административного регламента федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции ведения реестра операторов, осуществляющих обработку персональных данных».
4. Настоящим Положением, Положением о порядке организации и проведения работ по защите конфиденциальной информации в ГБУЗ «ГПТД» и другими локальными актами ГБУЗ «КПТД».
3.9.2. Приказом главного врача ГБУЗ «ГПТД» определяется:
- Ответственный за организацию обработки персональных данных;
- Перечень автоматизированных систем, в которых обрабатываются персональные данные;
- Перечень сотрудников (должностей сотрудников), допущенных к персональным данным, и объем персональных данных, к которым они допускаются;
- Перечень персональных данных, обрабатываемый в информационной системе персональных данных.
3.9.3. С целью определения угроз безопасности персональных данных при обработке в информационных системах ГБУЗ «ГПТД» должна быть проведена их классификация.
3.9.4. Должна быть разработана модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, которая утверждается главным врачом ГБУЗ «ГПТД».
3.9.5. В соответствии с классом информационной системы и моделью угроз безопасности персональных данных должны быть приняты меры в части технической защиты конфиденциальной информации. Информационные системы до начала обработки персональных данных должны пройти процедуру оценки эффективности принятых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.
3.9.6. В информационных системах персональных данных должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.
3.9.7. В информационных системах персональных данных должны быть предусмотрены меры для предотвращения внедрения вредоносных программ (программ-вирусов) и программных закладок.

3.9.8. При взаимодействии информационных систем персональных данных с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования), должны применяться следующие методы и способы защиты информации от несанкционированного доступа:
- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее передаче по каналам связи;
-использование смарт-карт, электронных замков и других носителей информации для надежной информации и аутентификации граждан;
- использование средств антивирусной защиты.
3.9.9. До начала обработки (в процессе обработки при наличии изменений) персональных данных направить в уполномоченный орган по защите прав субъектов персональных данных:
- уведомление о своем намерении осуществлять обработку персональных данных;
- фамилию, имя, отчество физического лица, ответственного за организацию обработки персональных данных, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;
Сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

3.10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут предусмотренную законодательством РФ ответственность (Приложение 3).

Приложение 1

Типовая форма

письменного согласия гражданина
на обработку персональных данных

СОГЛАСИЕ

Я, (фамилия, имя, отчество субъекта или его представителя)
_____
Адрес субъекта персональных данных (его представителя):
_____
_____
номер основного документа, удостоверяющего личность субъекта персональных данных (его представителя) (паспорт, удостоверение и т.п.)
_____серия_____№_____
сведения о дате выдачи основного документа и выдавшем его органе
_____
_____
реквизиты доверенности или иного документа, подтверждающего полномочия представителя субъекта персональных данных
_____
В соответствии со ст.9 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных» своей волей и в своем интересе выражаю

ГБУЗ «Гайский противотуберкулезный диспансер» (Кувандыкский филиал), юридический адрес: Оренбургская область, г. Гай, ул. Комсомольская, 19,

согласие на обработку моих персональных данных с целью (указать цель обработки):
- (указать перечень ВСЕХ персональных данных), включая любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распределение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Согласие вступает в силу со дня подписания и действует до (указать срок окончания обработки персональных данных). Обработка персональных данных прекращается на основании письменного заявления, если иное не предусмотрено Федеральным законом.
«___»_____20___г. Подпись

Приложение 2

Типовая форма

письменного согласия сотрудника
на обработку персональных данных

СОГЛАСИЕ

Я, (фамилия, имя, отчество субъекта или его представителя)

_____

адрес субъекта персональных данных (его представителя):

_____

_____

номер основного документа, удостоверяющего личность субъекта персональных данных (его представителя) (паспорт, удостоверение и т.п.)

_____серия_____№_____

сведения о дате выдачи основного документа и выдавшем его органе

_____

_____

реквизиты доверенности или иного документа, подтверждающего полномочия представителя субъекта персональных данных

_____

В соответствии со ст.9 Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных» своей волей и в своем интересе выражаю

ГБУЗ «Гайский противотуберкулезный диспансер» (Кувандыкский филиал), юридический адрес: Оренбургская область, г. Гай, ул. Комсомольская, 19,

согласие на обработку моих персональных данных с целью формирования общедоступных источников персональных данных (справочников, адресных книг, информации в СМИ и на сайте организации), включая любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распределение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Согласие вступает в силу со дня подписания и действует до расторжения трудового договора. Обработка персональных данных прекращается на основании письменного заявления, если иное не предусмотрено Федеральным законом.

«___»_____20___г. Подпись

Приложение 3

Ответственность
за нарушение норм, регулирующих обработку и защиту персональных данных

Уголовная ответственность (Уголовный кодекс РФ)

Статья 137. Нарушение неприкосновенности частной жизни

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующимся произведении или средствах массовой информации – наказываются штрафом, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев.
2. Те же деяния, совершенные лицом с использованием своего служебного положения, наказываются штрафом в размере от ста до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев.

Статья 140. 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 лонной информации, если эти деяния причинили вред правам и законным интересам граждан, наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет.

Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом, наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.
2. Незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.
4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, наказываются лишением свободы на срок до десяти лет.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом, либо исправительными аботами на срок от шести месяцев до одного года либо лишением свободы на срок до двух лет.
2. То же деяние совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, наказывается штрафом в размере от ста тысяч до трехсот рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации

ЭВМ, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, наказывается лишением свободы на срок до четырех лет.

Статья 292. Служебный подлог.

1. Служебный подлог, т.е. внесение должностным лицом, а также государственным служащим органа местного самоуправления, не являющимся должностным лицом, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание, если эти деяния совершенны из корыстной или иной личной заинтересованности (при отсутствии признаков преступления, предусмотренного частью первой 292^1 настоящего Кодекса), наказываются штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до двух лет.
2. Те же деяния, повлекшие существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 292^1. Незаконная выдача паспорта гражданина Российской Федерации, а равно внесение заведомо ложных сведений в документы, повлекшее незаконное приобретение гражданства Российской Федерации.

1. Незаконная выдача должностным лицом или государственным служащим паспорта гражданина Российской Федерации иностранному гражданину или лицу без гражданства, а равно внесение должностным лицом, а также государственным служащим или служащим органом местного самоуправления, не являющимся должностным лицом, заведомо ложных сведений в документы, повлекшее незаконное приобретение гражданства Российской Федерации, наказываются штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной

деятельностью на срок до трех лет, либо лишением свободы на срок до пяти лет.

2. Неисполнение или ненадлежащее исполнение должностным лицом или государственным служащим своих должностных обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло незаконную выдачу паспорта гражданина Российской Федерации иностранному гражданину или лицу без гражданства либо незаконное приобретение гражданства Российской Федерации, наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Статья 293. Халатность

1. Халатность, т.е. неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло причинение крупного ущерба или существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.
2. То же деяние, повлекшее по неосторожности причинение тяжкого вреда здоровью или смерть человека, наказывается лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.
3. Деяние, предусмотренное частью первой настоящей статьи, повлекшее по неосторожности смерть двух и более лиц, наказывается лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Примечание. Крупным ущербом в настоящей статье признается ущерб, сумма которого превышает сто тысяч рублей.

Административная ответственность.

(Кодекс от Административных Правонарушениях РФ (КоАП РФ)

Статья 5.39. Отказ в предоставлении гражданину информации

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредоставление иной

информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации, влечет наложение административного штрафа на должностных лиц в размере от пятисот до одной тысячи рублей.

Статья 13.11. Нарушение установленного законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей.
2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от одной тысячи до двух тысяч рублей; на юридических лиц – от десяти тысяч до двадцати тысяч рублей с конфискацией несртифицированных средств защиты информации или без таковой.

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен Федеральным Законом «О персональных данных» (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, (ст.14.33 – недобросовестная конкуренция) влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц – от четырех тысяч до пяти тысяч рублей.

Статья 19.5. Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)

1. Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), об устранении нарушений законодательства – влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от одной тысячи до двух тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от десяти тысяч до двадцати тысяч рублей.
2. Невыполнение в установленный срок законного предписания, решения органа, уполномоченного в области экспортного контроля, его территориального органа – влечет наложение административного штрафа на должностных лиц в размере от пяти тысяч до десяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от двухсот тысяч до пятисот тысяч рублей.

Статья 19.7. Непредставление сведений.

Непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых не предусмотрено законом необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде, за исключением случаев, предусмотренных статьями 19.7^{1}, 19.7^{2}, 19.7^{3}, 19.8, 19.9 настоящего Кодекса, - влечет наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц – от трехсот до пятисот рублей; на юридических лиц – от трех тысяч до пяти тысяч рублей.

Дисциплинарная ответственность

(Трудовой Кодекс РФ)

Статья 81. Расторжение трудового договора по инициативе работодателя.

В) разглашения охраняемой законом тайны (государственной, коммерческой, служебной или иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекается к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами,

а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Статья 237. Возмещение морального вреда, причиненного работнику.

Моральный вред, причиненный работнику неправомерными действиями или бездействием работодателя, возмещается работнику в денежной форме в размерах, определяемых соглашением сторон трудового договора. В случае возникновения спора факт причинения работнику морального вреда и размеры его возмещения определяются судом независимо от подлежащего возмещению имущественного ущерба.