Департамент здравоохранения Тюменской области
Государственное бюджетное учреждение здравоохранения
Тюменской области
«Областная больница №14 имени В.Н. Шанаурина» (с.Казанское)

П Р И К А З

22 февраля 2023г. № 19 ос

с. Казанское

Об организации обработки и защиты персональных данных в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

В соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,**п р и к а з ы в а ю:**

1. Утвердить:

- положение об обработке и защите персональных данных в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 1 к настоящему приказу).
- перечень персональных данных, подлежащих защите в информационных системах персональных данных ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 2 к настоящему приказу).
- инструкцию по обеспечению информационной безопасности при работе пользователей с информационными системами ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 3 к настоящему приказу).
- регламент по организации доступа в информационно-телекоммуникационную сеть «Интернет» и работе с электронной почтой пользователей локальных вычислительных сетей, входящих в состав корпоративной сети передачи данных ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 4 к настоящему приказу).
- положение об антивирусной защите информационных систем и рабочих станций пользователей ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 5 к настоящему приказу).

- инструкцию о предоставлении прав доступа к защищаемым информационным ресурсам ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 6 к настоящему приказу).
- инструкцию по организации парольной защиты информационных систем и рабочих станций пользователей ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 7 к настоящему приказу).
- инструкцию по предоставлению допуска сторонним организациям для проведения работ в информационных системах ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 8 к настоящему приказу).
- инструкцию о порядке проверки электронного журнала обращений в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 9 к настоящему приказу).
- правила рассмотрения запросов субъектов персональных данных или их представителей в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 10 к настоящему приказу).
- инструкцию по обработке персональных данных без использования средств автоматизации в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (Приложение № 11 к настоящему приказу).

2. Ознакомить всех сотрудников, задействованных в обработке персональных данных с настоящим приказом.

3. Контроль за исполнением настоящего приказа возложить на заместителя главного врача.

Главный врач Д.М. Суворов

Приложение № 1
Утверждено
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Положение
об обработке и защите персональных данных в
ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Общие положения

1.1. Настоящее положение по обработке персональных данных в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее - Положение) разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом 27 июля 2006 года№ 152-ФЗ«О персональных данных», Правилами внутреннего трудового распорядка ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее –Учреждение).

1.2 Цель разработки Положения - определение порядка обработки персональных данных работников Учреждения и иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий оператора; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника Учреждения, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2. Основные понятия

Для целей настоящего Положения используются следующие понятия:

2.1. Оператор персональных данных (далее оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. В рамках настоящего положения оператором является - ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское).

2.2. 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, состояний здоровья, другая информация о физическом лице.

2.3. Субъект – субъект персональных данных.

2.4. 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.

2.5. Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.6. Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении Субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы Субъекта персональных данных или других лиц.

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

2.8. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

3. Обработка персональных данных

3.1. Общие требования при обработке персональных данных.

В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных обязаны соблюдаться следующие требования:

3.1.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения Конституции Российской Федерации, законов и иных нормативных правовых актов Российской Федерации, содействия Субъектам персональных данных в трудоустройстве, продвижении по службе, обучении, контроля количества и качества выполняемой работы, обеспечения личной безопасности Субъекта персональных данных и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества оператора.

3.1.2. Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

3.1.3. При принятии решений, затрагивающих интересы Субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.4. Субъекты персональных данных имеют право ознакомиться с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

3.2. Получение персональных данных:

3.2.1. Все персональные данные следует получать непосредственно от Субъекта персональных данных. Субъект самостоятельно принимает решение о предоставление своих персональных данных и дает согласие на их обработку оператором.

3.2.2. Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

3.2.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

3.2.4. В случаях, когда оператор может получить необходимые персональные данные Субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа Субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из которых предоставляется субъекту, второй хранится у оператора.

3.2.5. Запрещается получать и обрабатывать персональные данные Субъекта о его политических, религиозных и иных убеждениях и частной жизни.

3.2.6. Запрещается получать и обрабатывать персональные данные Субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.3. Хранение персональных данных:

3.3.1. Хранение персональных данных субъектов осуществляется соответствующими структурными подразделениями оператора.

3.3.2. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положения об особенностях обработки персональных данных. Осуществляемой без использования средств автоматизации», утвержденного постановлением Правительства Российской Федерациот 15 сентября 2008 г. № 687.

3.4. Передача персональных данных:

3.4.1. При передаче персональных данных Субъекта оператор обязан соблюдать следующие требования:

– не сообщать персональные данные Субъекта третьей стороне без письменного согласия Субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами;

– предупредить лиц, получающих персональные данные Субъекта, 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 Субъекта, обязаны соблюдать требования конфиденциальности;

– не сообщать персональные данные Субъекта в коммерческих целях без его письменного согласия;

– запрашивать сведения о состоянии здоровья Субъекта, относящиеся к вопросу о возможности выполнения оператором своих функций;

– все сведения о передаче персональных данных Субъекта регистрируются в целях контроля правомерности использования данной информации лицами, ее получившими с фиксацией сведений о лице, направившем запрос, даты передачи персональных данных или даты уведомления об отказе в их предоставлении, а также с отметкой какая именно информация была передана.

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

3.4.3. Внутренний доступ (доступ внутри организации) к персональным данным Субъекта. Право доступа к персональным данным Субъекта имеют:

– главный врач;
– заместители главного врача;
– врачи в пределах своих функциональных обязанностей;
– медицинские сестры в пределах своих функциональных обязанностей;
– сотрудники регистратуры в пределах своих функциональных обязанностей;
– сотрудники отдела кадров в пределах своих функциональных обязанностей;
– сотрудники отдела бухгалтерского учета в пределах своих функциональных обязанностей;
– сам субъект, носитель данных.

3.4.4. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать обязательство о неразглашении персональных данных.

3.4.5. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры:

– налоговые инспекции;
– правоохранительные органы;
– органы статистики;
– страховые агентства;
– военкоматы;
– органы социального страхования;
– пенсионные фонды;

– подразделения федеральных, республиканских и муниципальных органов управления.

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

3.5. Уничтожение персональных данных:

3.5.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки и Законодательство Российской Федерации, они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.5.2. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

4. Права и обязанности субъектов персональных данных и оператора

4.1. В целях обеспечения защиты персональных данных Субъекты имеют право:

– получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

– осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных Федеральным Законом;

– требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением Законодательства;

– при отказе оператора или уполномоченного им лица исключить или исправить персональные данные Субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

– дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;

– требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта, обо всех произведенных в них изменениях или исключениях из них;

– обжаловать в суде любые неправомерные действия или бездействие оператора, или уполномоченного им лица при обработке и защите персональных данных Субъекта.

4.2. Для защиты персональных данных Субъектов оператор обязан:

– за свой счет обеспечить защиту персональных данных Субъекта от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации;

– ознакомить Субъекта с настоящим положением и его правами в области защиты персональных данных любым общедоступным способом;

– осуществлять передачу персональных данных Субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

– предоставлять персональные данные Субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их обязанностей в соответствии с настоящим положением и законодательством Российской Федерации;

– обеспечить субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

– по требованию Субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

4.3. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

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

5.1. Оператор несет ответственность за надлежащую обработку персональных данных.

5.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к ответственности в порядке, установленном Законодательством Российской Федерации.

Приложение № 2
Утвержден
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Перечень
персональных данных, подлежащих защите в информационных системах персональных данных ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Настоящий Перечень персональных данных, подлежащих защите в информационных системах персональных данных ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее –Перечень), разработан в соответствии с рекомендациями Министерством здравоохранения Российской Федерации.

Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (далее – СЗПДн).

1. Общие положения

Объектами защиты являются – информация, обрабатываемая в информационных системах персональных данных (далее – ИСПДн), и технические средства ее обработки и защиты.

Объекты защиты каждой ИСПДн включают:

а) Обрабатываемая информация:
- персональные данные (далее – ПДн) Субъектов(раздел 2.1.1);
- ПДн сотрудников (раздел 2.1.2).

б) Технологическая информация (раздел 2.2).

в) Программно-технические средства обработки (раздел 2.3).

г) Средства защиты ПДн (раздел 2.4).

д) Каналы информационного обмена и телекоммуникации (раздел 2.5).

е) Объекты и помещения, в которых размещены компоненты ИСПДн (раздел 2.6).

2. ИСПДн

2.1. Обрабатываемая информация

2.1.1. Перечень персональных данных субъектов ПДн

Персональные данные Субъектов (пациентов) включают:

а) Фамилия, имя, отчество;

б) дата рождения;

в) контактный телефон;

г) адрес прописки;

д) адрес фактического проживания;

е) паспортные данные;

ж) данные о состоянии здоровья (история болезни).

2.1.2. Перечень ПДн сотрудников Учреждения

ПДн сотрудников Учреждения включают:

а) Фамилия, имя, отчество;

б) место, год и дата рождения;

в) адрес по прописке;

г) паспортные данные (серия, номер паспорта, кем и когда выдан);

д) информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);

е) информация о трудовой деятельности до приема на работу;

ж) информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);

з) адрес проживания (фактический);

и) телефонный номер (домашний, рабочий, мобильный);

к) семейное положение и состав семьи (муж/жена, дети);

л) информация о знании иностранных языков;

м) форма допуска;

н) оклад;

о) Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);

п) сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

р) ИНН;

с) данные об аттестации работников;

т) данные о повышении квалификации;

у) данные о наградах, медалях, поощрениях, почетных званиях;

ф) информация о приеме на работу, перемещении по должности, увольнении;

х) информация об отпусках;

ц) информация о командировках;

ч) информация о болезнях;

ш) информация о негосударственном пенсионном обеспечении.

2.2. Технологическая информация

Технологическая информация, подлежащая защите, включает:

а) управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);

б) технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);

в) информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

г) информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;

д) информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

е) служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки обрабатываемой информации.

2.3. Программно-технические средства обработки

Программно-технические средства включают в себя:

а) общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);

б) резервные копии общесистемного программного обеспечения;

в) инструментальные средства и утилиты систем управления ресурсами ИСПДн;

г) аппаратные средства обработки ПДн (АРМ и сервера);

д) сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы).

2.4. Средства защиты ПДн

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

а) средства управления и разграничения доступа пользователей;

б) средства обеспечения регистрации и учета действий с информацией;

в) средства, обеспечивающие целостность данных;

г) средства антивирусной защиты;

д) средства межсетевого экранирования;

е) средства анализа защищенности;

ж) средства обнаружения вторжений;

з) средства криптографической защиты ПДн, при их передаче по каналам связи сетей общего и (или) международного обмена.

2.5. Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

2.6. Объекты и помещения, в которых размещены компоненты ИСПДн

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

Приложение № 3
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Инструкция
по обеспечению информационной безопасности при работе пользователей с информационными системами ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Информационные ресурсы, хранящиеся в электронном виде в информационных системах (далее - ИС) Учреждения на магнитных, оптических и иных носителях информации, являются собственностью ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское). Все без исключения работники Учреждения, а также представители внешних организаций, допущенные к данным информационным ресурсам и участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и данным автоматизированной системы (далее - пользователи), несут персональную ответственность за свои действия.

Пользователи **обязаны:**

1. использовать информационные ресурсы предприятия только для выполнения своих функциональных обязанностей в соответствии с положением о структурном подразделении, своими должностными инструкциями;
2. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;
3. знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;
4. хранить в тайне свой пароль (пароли), с установленной периодичностью менять свой пароль (пароли);
5. выполнять требования по антивирусной защите в ИС в части, касающейся действий пользователей рабочих станций[1] (далее - РС) ИС;
6. присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним РС;
7. немедленно вызывать администратора безопасности (ответственного за соблюдение информационной безопасности ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) и ставить в известность руководителя подразделения в следующих случаях:

[1] Рабочая станция - персональный компьютер пользователя ИС, включающий в свой состав системный блок, монитор, клавиатуру, оптический манипулятор, набор программного обеспечения. Дополнительно может комплектоваться другими периферийными устройствами

а) нарушения целостности пломб, наклеек, нарушения или несоответствия номеров печатей на аппаратных средствах РС или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищенной РС;

б) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств РС;

в) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию РС, выхода из строя или неустойчивого функционирования узлов РС или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

г) некорректного функционирования установленных на РС технических средств защиты;

д) обнаружения непредусмотренных кабельных отводов и устройств, подключенных к РС.

Пользователям **запрещается:**

1. использовать компоненты программного и аппаратного обеспечения ИС Учреждения в неслужебных целях;
2. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств РС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные конфигурациями рабочих станций;
3. самовольно производить сборку, разборку, установку и техническое обслуживание аппаратных средств;
4. осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
5. записывать и хранить информацию, являющуюся конфиденциальной, на неучтенных носителях информации (гибких магнитных дисках, оптических дисках, флэш-картах и т.п.);
6. оставлять включенной без присмотра свою РС, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана);
7. отключать средства защиты и использовать не согласованные с администратором безопасности режимы их функционирования;
8. осуществлять поиск способов преодоления установленной аппаратно - программной защиты информации, а также использовать аппаратно - программные средства, реализующие названные способы;
9. разглашать информацию, открывающую доступ для других лиц к техническим средствам и данным или передавать кому-либо средства доступа к ним;
10. умышленно использовать недокументированные особенности и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок пользователи обязаны ставить в известность администратора безопасности (ответственного за безопасность информации) и руководителя своего структурного подразделения.

Приложение № 4
Утвержден
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Регламент
по организации доступа в информационно-телекоммуникационную сеть «Интернет» и работе с электронной почтой пользователей локальных вычислительных сетей, входящих в состав корпоративной сети передачи данных ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Доступ пользователей к сети Интернет

1.1. Решение о служебной необходимости подключения пользователя к сети Интернет принимает руководитель структурного подразделения, в которое принят пользователь.

Подключение к сети Интернет и электронной почте пользователей локально - вычислительных сетей (далее - ЛВС) производится на основании письменной заявки на заместителя главного врача.

1.2. Учреждение контроля за соблюдением правил доступа в сеть Интернет и работы с электронной почтой возлагается на руководителей структурных подразделений при осуществлении технической поддержки администратора информационной безопасности.

1.3. Пользователь обязан использовать сеть Интернет только для выполнения своих служебных обязанностей в соответствии с должностной инструкцией и заданием непосредственного руководителя.

2. **Обязанности пользователя сети Интернет**

2.1. Сохранять в тайне парольно - ключевую информацию, позволяющую осуществлять доступ в сеть Интернет.

2.2. При получении по электронной почте подозрительных сообщений с вложениями, удалять их не открывая.

2.3. Ставить в известность непосредственного руководителя и администратора ЛВС, либо администратора безопасности о возможных попытках несанкционированного доступа извне к компьютеру, появляющихся нештатных ситуациях при работе программных средств, а также в иных случаях, указывающих на возможность злонамеренных действий извне.

3. **Обязанности пользователя при работе с электронной почтой**Пользователи обязаны использовать электронную почту только для выполнения своих служебных обязанностей.

3.2. Сохранять в тайне парольно – ключевую информацию, позволяющую осуществить доступ к электронному почтовому ящику пользователя.

3.3. При получении электронных сообщений сомнительного содержания, сообщений с незнакомых адресов, а также сообщений с известных пользователю адресов, но вызывающих сомнения в их содержимом, пользователю запрещается открывать вложенные файлы, так как они могут содержать вирусы, либо вредоносные программы.

4. **Пользователю сети Интернет и электронной почты запрещается:**

4.1. Отвечать на подозрительные письма и сообщать любые данные о себе.

4.2. Передавать, используя сеть Интернет и электронную почту информацию, входящую в перечень сведений конфиденциального характера Учреждения.

4.3. Передавать кому-либо, а также записывать на видном месте пароль доступа к своему почтовому ящику.

4.4. Рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а так же ссылки на вышеуказанную информацию.

4.5. Распространять и использовать по собственной инициативе загруженные из сети Интернет или полученные по электронной почте программные продукты и иные материалы, не связанные с производственной деятельностью (компьютерные игры, тексты и т.п.).

4.6. Пытаться самостоятельно преодолеть установленные ограничения доступа к ресурсам Интернет, в том числе с использованием специальных программ.

4.7. Устанавливать на АРМ (РС), используемом для доступа в сеть Интернет . программное обеспечение, обладающее функциями перехвата информации, в том числе серверов-посредников прикладного уровня, и специализированное программное обеспечение, позволять осуществлять трансляцию IP-адресов.

4.8. Осуществлять массовую рассылку (15 и более адресов) сообщений по электронной почте в сети Интернет без письменного согласования с руководителем структурного подразделения.

4.9. Использовать адрес электронной почты для оформления подписок, не имеющих отношение к трудовой деятельности пользователя.

4.10. Распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну,

копирайт или прочие права собственности и/или авторские и смежные с ними права третьей стороны.

4.11. Распространять информацию противозаконного, экстремистского, характера, запрещенную международным и Российским законодательством, включая материалы непристойного и порнографического характера, а также информацию, оскорбляющую честь и достоинство других лиц, материалы способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

5. **Ответственность пользователя**

5.1. Пользователи сети Интернет и электронной почты несут дисциплинарную и иную ответственность за несоблюдение требований настоящего регламента в соответствии с действующим законодательством Российской Федерации.

5.2. За преднамеренные действия, повлекшие порчу или уничтожение информации, неправомерный доступ к охраняемой законом информации, создание и использование вредоносных программ пользователи могут быть привлечены к уголовной ответственности.

5.3. В случае нарушений данного регламента доступ в сеть Интернет с компьютера пользователя, допустившего нарушение, блокируется. Возобновление доступа осуществляется после предоставления пользователем объяснительной записки по данному нарушению, завизированной его непосредственным руководителем.

5.4. В случае неоднократных нарушений настоящего регламента доступ в сеть Интернет с использованием учетной записи пользователя, допустившего нарушения блокируется на неопределенный срок и Администратором информационной безопасности направляется служебная записка на имя руководителя структурного подразделения пользователя, допустившего нарушения с предложением о дисциплинарном взыскании данного лица.

Приложение № 5
Утверждено
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Положение
об антивирусной защите информационных систем и рабочих станций пользователей ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Общие положения

1.1. Система антивирусной защиты информации предназначена для предотвращения заражения программными вирусами информационных систем и автоматизированных рабочих мест пользователей корпоративной сети передачи данных (далее - КСПД).

1.2. Антивирусная защита информации осуществляется посредством применения организационных мер, а также технических средств антивирусной защиты информации.

1.3. Требования настоящего Положения обязательны для выполнения всеми должностными лицами и работниками Учреждения.

2. Организационная структура системы антивирусной защиты информации:

2.1. Учреждение антивирусной защиты, анализ ее состояния, осуществляется администратором информационной безопасности.

2.2. Выполнение мероприятий по организации антивирусной защиты информации на рабочих станциях пользователей осуществляет администратор антивирусной защиты (далее - администратор АВЗ), назначаемый приказом с отражением этих обязанностей в должностной инструкции. Выполнение указанных мероприятий в части серверного оборудования осуществляется в присутствии администратора данного сервера.

2.3. Администратор АВЗ несет ответственность:

- за своевременную инсталляцию средств антивирусной защиты информации;
- за правильную эксплуатацию средств антивирусной защиты информации;
- за обновление баз данных средств антивирусной защиты на рабочих местах пользователей.

2.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на серверах несет администратор данных серверов.

2.5. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах несут пользователи.

2.6. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;
- самостоятельно устанавливать на служебные персональные компьютеры любое программное обеспечение.

2.7. Пользователям рекомендуется:

- не создавать самораспаковывающиеся архивы;
- использовать для хранения офисных документов форматы файлов, не содержащих кодов макрокоманд HTML, RTF и др.

2.8. Нелегальное распространение и/или установка антивирусного программного обеспечения запрещена. За несанкционированное распространение средств антивирусной защиты виновные несут ответственность в соответствии с законодательством Российской Федерации.

3. Порядок применения средств антивирусной защиты информации

3.1. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на машинных носителях информации;
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в месяц) и обязательная проверка используемых в работе съемных накопителей (флэш-карты) перед началом работы с ними;
- внеплановая проверка магнитных носителей информации в случае подозрения на наличие программных вирусов;
- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

3.2. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, серверном оборудовании, в том числе на серверах баз данных, почтовых серверах, рабочих станциях.

3.3. На рабочем месте администратора АВЗ должны быть установлены средства, позволяющие на расстоянии управлять компонентами системы антивирусной защиты информации, установленными на рабочих станциях и серверах сегментов локальных вычислительных сетей.

3.4. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

4. Действия при обнаружении программных вирусов

4.1. В случае обнаружения программных вирусов пользователь должен:

- прекратить процесс приема-передачи информации;
- сообщить администратору АВЗ и ответственному о факте обнаружения программного вируса;
- принять меры для локализации и удаления программных вирусов с использованием средств антивирусной защиты информации;
- сообщить о факте обнаружения программных вирусов отправителю, от которого поступили зараженные гибкие магнитные носители, файлы или почтовые сообщения.

Приложение № 6
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени В.Н.
Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Инструкция
о предоставлении прав доступа к защищаемым информационным ресурсам ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Настоящая инструкция регламентирует порядок предоставления сотрудниками Учреждения прав доступа к информационным системам, подлежащим защите.

Каждому сотруднику, допущенному к работе с конкретной информационной системой (далее - ИС) ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) предоставляется персональное уникальное имя (логин, учетная запись), под которым он регистрируется и получает доступ к ресурсам ИС. Авторизация пользователя в информационной системе может осуществляться, как с полномочиями учетной записи домена, так и дополнительных учетных записей для каждой ИС.

Не допускается использование несколькими работниками одного и то же имени пользователя при работе с ИС, передача кому-либо своих учетных записей, а также работа с ИС с использованием чужих учетных записей.

Регистрация работника и предоставление ему прав доступа для работы в информационной системе производится по письменному заявлению руководителя структурного подразделения, в котором работает данный работник.

На основании согласованного заявления ответственный администратор ИС заводит данные пользователя в систему.

Учетные записи всех пользователей должны быть «привязаны» к конкретным рабочим станциям (MAC - адресам их сетевых карт) или к сегменту (группе) рабочих станций.

Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в квартал.

Централизованный учет сведений о защищаемых ресурсах ведет администратор вычислительных сетейГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское).

Приложение № 7
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени
В.Н. Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Инструкция
по организации парольной защиты информационных систем и рабочих станций пользователей ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское), а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

1. Требования к генерации паролей:

– обязательная длина пароля – не менее - 6 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $,&,*,% и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, цифровые значения даты рождения и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, TESTи т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

– личный пароль пользователь не имеет права сообщать никому, в том числе администратору информационной системы;

– длина пароля администратора информационной системы должна быть не менее 10 символов.

2. Пароли административного доступа к телекоммуникационному оборудованию, входящему в состав КСПД генерируются централизованно.

3. Плановая смена паролей администраторов и пользователей должна проводиться регулярно, не реже одного раза в квартал.

4. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на работу в другое подразделение организации и т.п.) должна производиться администраторами немедленно после окончания последнего сеанса работы данного пользователя с системой.

5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое подразделение организации со снятием соответствующих обязанностей др.) администраторов или других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой

подсистем автоматизированной системы ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское).

6. Хранение сотрудником значений своих паролей на бумажном носителе, либо записанные иным доступным способом, позволяющим их прочитать не допускается.

7. Контроль за действиями пользователей по парольной защите возлагается на администратора вычислительных сетейГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское).

Приложение № 8
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени
В.Н. Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Инструкция
по предоставлению допуска сторонним организациям для проведения работ в информационных системах ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. **Общие положения**

1.1. Настоящая Инструкция определяет порядок проведения работ в информационных системах ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее - ИС)работниками сторонних организаций.

1.2. Допуск работников сторонних организаций в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) осуществляется в соответствии с установленным пропускным режимом, при наличии документов, удостоверяющих личность.

1.3. Работники сторонних организаций, допущенные для проведения работ с информационными системами, должны выполнять принятые в Учреждении требования по обеспечению режима конфиденциальности информации, информационной безопасности, правила охраны труда, правила технической эксплуатации электроустановок потребителей, правила пожарной безопасности.

2. **Основание допуска к работам**

2.1. Наличие подписанного сторонами договора подряда (субподряда) на выполнение монтажных, пуско-наладочных, ремонтных, восстановительных работ, либо договора на обслуживание программного обеспечения или оборудования.

2.2. Наличие соглашения о конфиденциальности между Учреждением и сторонними организациями, допущенными к работам на территории ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское), если в ходе работ указанные организации получают доступ к сведениям, составляющим коммерческую тайну или информацию конфиденциального характера.

3. **Регламентирование проведения работ**

3.1. Допуск работников сторонних организаций в помещения, в которых установлено оборудование аппаратного обеспечения информационных систем, а также оборудование систем связи и телекоммуникаций, разрешается только с сопровождающим, являющимся ответственным за работоспособность данного оборудования.

3.2. Ответственность за соблюдение требований по внутри-объектовому режиму, режиму конфиденциальности, информационной безопасности, охране труда, пожарной безопасности в ходе проведения работ возлагается на руководителей структурных подразделений предприятия, на объектах которых проводятся работы.

3.3. Монтажные, ремонтные, наладочные работы, работы связанные с подключением электроустановок Учреждения персоналом сторонних организаций должны производиться в соответствии с Правилами по охране труда при эксплуатации электроустановок (утверждены Приказом Минтруда России от 24.07.2013 N 328н), инструкциями по охране труда.

4. В ходе проведения работ запрещается:

– производство подключений (инсталляция) к информационным системам, а также к системе информационной безопасности и системам связи и телекоммуникаций, непредусмотренных проектом (заданием, договором) программно-технических средств, в том числе нелицензионного программного обеспечения;

– бесконтрольное перемещение работников сторонних организаций по территории проведения работ.

Приложение № 9
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени
В.Н. Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19 ос

Инструкция
о порядке проверки электронного журнала обращений
в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина»
(с. Казанское)

1. Общие положения

1.1.Инструкция о порядке проверки электронного журнала обращений в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – инструкция) определяет порядок проверки электронных журналов обращений к ресурсам информационных систем персональных данных (далее – ИСПДн) в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское) (далее – Учреждение).

1.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

1.3. Право проверки электронного журнала обращений имеют:

- администратор информационной безопасности;
- ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн;
- заместитель главного врача.

2. Порядок проверки электронного журнала

2.1 На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее – СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

2.2 Проверке подлежат все электронные журналы ИСПДн

2.3 Проверка должна проводиться не реже чем один раз в неделю с целью своевременного выявления фактов нарушения требований положения об обработки ПДн Учреждения.

2.4 Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки администратор информационной безопасности делает соответствующую отметку в журнале и ставит свою роспись.

Приложение № 10
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени
В.Н. Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19ос

Инструкция
правила рассмотрения запросов субъектов персональных данных или их представителей в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Общие положения

Настоящий документ устанавливает правила рассмотрения запросов субъектов персональных данных или их представителей направленных на предотвращение нарушений законодательства Российской Федерации при обработке персональных данных, определяет сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований регламентирует порядок работы с документами и электронными и магнитными носителями, содержащими персональные данные ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) (далее – Учреждение), в целях реализации: Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Постановление Правительства Российской Федерации от 01.11.2012№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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 правыми актами, операторами, являющимися государственными или муниципальными органами».

2. Порядок рассмотрения запросов субъектов персональных данных или их представителей

2.1. В целях обеспечения сохранности документов, содержащих персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться сотрудниками Учреждения, осуществляющими данную работу в соответствии:

– со своими служебными обязанностями, зафиксированными в их должностных регламентах (инструкциях);

– с Правилами обработки персональных данных в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское).

2.2. Запросы, поступающие в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское) обрабатываются в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и с утвержденной инструкцией по ведению делопроизводства в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с.Казанское). При обработке документа, содержащего персональные данные, в книге учета входящих/исходящих расписываются все сотрудники Учреждения, участвующие в работе с этим документом. Документ выдается сотрудникам, допущенным к работе с персональными данными.

2.3. Ответ на запрос предоставляется только при наличии обоснованной причины в соответствии с законодательством Российской Федерации, документа, удостоверяющего личность (с наличием фото), а при необходимости доверенности заверенной нотариусом.

2.4. Ответы на запросы граждан и организаций даются в объеме полученного запроса, за исключением данных, содержащихся в материалах запроса или опубликованных в общедоступных источниках.

2.5. Жалобы субъектов персональных данных (в том числе в электронном виде) на нарушение прав в области незаконного использования их персональных данных, оформленные в соответствии с требованиями, установленными законодательством (примерная форма жалобы Субъекта персональных данных - Приложение №1) и регистрируются в журнале регистрации и учета обращений субъектов персональных данных (Приложение №2).

2.6. Лицо, ответственное за организацию обработки персональных данных, несет ответственность за организацию приема и обработки обращений и запросов субъектов персональных данных или их представителей по нарушению прав в области незаконного использования их персональных данных и осуществляет контроль за приемом и обработкой таких обращений и запросов.

Приложение № 1
к Правилам рассмотрения запросов
субъектов персональных данных или
их представителей в ГБУЗ ТО
Областная больница №14 имени
В.Н. Шанаурина» (с.Казанское)

Примерная форма
жалобы Субъекта персональных данных

от _____№ _____

В *ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)*

Жалоба

Ф.И.О:

_____

(местонахождение заявителя (фактический адрес)

_____

_____

Почтовый адрес, адрес электронной почты (по которому должен быть дан ответ)

_____

_____

Суть жалобы: _____

Перечень прилагаемых документов (прилагаются в случае необходимости)

М.П. _____ дата _____

Подпись заявителя

Приложение № 2
к Правилам рассмотрения запросов субъектов
персональных данных или их представителей
в ГБУЗ ТО Областная больница №14 имени
В.Н. Шанаурина» (с.Казанское)

Типовая форма
журнала регистрации и учета обращений субъектов персональных данных
в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

Журнал начат _____ _____
Журнал завершен _____ _____
Ответственный _____ (Ф.И.О.)
На _____ листах

№ п/п	Дата обращения	Номер входящего документа	Цель обращения	Ф.И.О. работника, принявшего обращение	Действия по результатам обращения	Примечание

Приложение № 11
Утверждена
приказом ГБУЗ ТО Областная
больница №14 имени
В.Н. Шанаурина» (с.Казанское)
от «22» февраля 2023 г. № 19ос

Инструкция
по обработке персональных данных без использования средств автоматизации в ГБУЗ ТО Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)

1. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

1.1. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

1.2. К обработке персональных данных могут иметь доступ сотрудники Учреждения, определённые приказом, при этом они должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

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

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержаться в информационной системе персональных данных либо были извлечены из нее.

1.4. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных.

Согласие Субъекта персональных данных не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании Федерального закона Российской Федерации, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные

данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи;

5) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе кандидатов на выборные муниципальные должности;

6) в иных случаях, определённых Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

1.5. Хранение персональных данных должно происходить в порядке, исключающем их утрату, неправомерное использование, распространение (в том числе передачу) без согласия Субъекта персональных данных и несанкционированный доступ.

1.6. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных, в специальных разделах или на типовых формах документов.

1.7. Сотрудники, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть ознакомлены с настоящей инструкцией.

1.8. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

1.9. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес Субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на

обработку персональных данных, осуществляемую без использования средств автоматизации - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

1.10. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

1.11. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

1.12. Уточнение персональных данных 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.

2. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

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

2.2. Сотрудник при работе с персональными данными обязан:

2.1. принимать необходимые меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

2.2. предоставлять информацию субъекту персональных данных при его обращении, касающейся обработки персональных данных, в том числе содержащей:

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

б) способы обработки персональных данных;

в) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

г) перечень обрабатываемых персональных данных и источник их получения;

д) сведения о том, какие юридические последствия может повлечь за собой обработка его персональных данных.

2.3. осуществить блокирование персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора;

2.4. устранять допущенные нарушения в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления.

2.5. сообщать непосредственному начальнику о попытках несанкционированного доступа к персональным данным.

<u>ЛИСТ ОЗНАКОМЛЕНИЯ</u>

с приказом ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина»
(с.Казанское)
«Об организации обработки и защиты персональных данных
в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина»
(с. Казанское)»

от___________________ №______

ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина» (с.Казанское)

№ п/п	Ф.И.О.	Должность	Подпись	Дата

ЛИСТ ОЗНАКОМЛЕНИЯ
с приказом ГБУЗ ТО «Областная больница № 14 имени В.Н.Шанаурина» (с.Казанское)

««Об организации обработки и защиты персональных данных в ГБУЗ ТО «Областная больница №14 имени В.Н. Шанаурина» (с. Казанское)»

от____________________ №_____

Филиал №1 Сладковская районная больница:

№ п/п	Ф.И.О.	Должность	Подпись	Дата