Государственное автономное учреждение здравоохранения
Тюменской области
«ГОРОДСКАЯ ПОЛИКЛИНИКА № 3»

ПРИКАЗ

«30» декабря 2022 г. № 483-п

г. Тюмень

Об утверждении требований по обеспечению
безопасности персональных данных
при их обработке в ИСПД

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить:
1.1. прилагаемые требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерский и кадровый учет»; информационной системе персональных данных «ИС УРМО ТО»; информационной системе персональных данных «Обращения граждан» (Приложение №1);
1.2. типовую форму согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (далее – Согласие) в ГАУЗ ТО «Городская поликлиника №3» (Приложение №2);
1.3. типовую форму соглашения о неразглашении информации, содержащую персональные данные в ГАУЗ ТО «Городская поликлиника №3» (Приложение №3).
2. Назначить ответственным за:
2.1. организацию обработки персональных данных начальника организационно-методического отдела – Белкина Игоря Леонидовича;
2.2. за эксплуатацию ИСПДн «Бухгалтерский и кадровый учет» Мурашову Любовь Геннадьевну – начальника отдела по управлению персоналом;
2.3. за эксплуатацию ИСПДн «ИС УРМО ТО» системного администратора информационно – коммуникационных сетей Овчарова Алексея Владимировича;
2.4. за эксплуатацию ИСПДн «Обращения граждан»: Молозину Галину Васильевну – заведующего сектором медицинской статистики.
3. Ответственным за эксплуатацию ИСПДн в рамках трудовой деятельности:
3.1. руководствоваться локальными нормативными актами, регламентирующими требования по обеспечению безопасности персональных данных при из обработке в информационных системах;
3.2. обеспечить наличие подписанного обязательства о неразглашении информации, содержащей персональные данные и согласия на обработку персональных данных,

разрешенных субъектом персональных данных для распространения всех сотрудников ГАУЗ ТО «Городская поликлиника №3».

4. Начальнику организационно-методического отдела Белкину И.Л. ознакомить всех заинтересованных сотрудников, задействованных в обработке персональных данных с настоящим приказом.
5. Приказ № 6-пд от 09.01.2019 «Об утверждении требований по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных» считать утратившим силу.
6. Контроль исполнения приказа возложить на заместителя главного врача Семенову К.А.

Главный врач С. И. Нагибин

Приложение № 1 к приказу
ГАУЗ ТО «Городская поликлиника №3»
от «30» декабря 2022 г. № 483-п

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерский и кадровый учет»

1. Общие положения

1. Данные требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (далее – ИСПДн) «Бухгалтерский и кадровый учет», ИСПДн «Обращения граждан», ИСПДн «ИС УРМО ТО» ГАУЗ ТО «Городская поликлиника №3» (далее – Требования) разработаны на основании:

1.1. приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

1.2. частной модели угроз безопасности ПДн при их обработке в ИСПДн;

1.3. акта определения уровня защищенности ПДн при их обработке в ИСПДн;

1.4. приказа ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

2. Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности персональных данных (далее – ПДн) при их обработке в ИСПДн «Бухгалтерский и кадровый учет», ИСПДн «Обращения граждан», ИСПДн «ИС УРМО ТО» ГАУЗ ТО «Городская поликлиника №3».

2. Организационные мероприятия по обеспечению безопасности ПДн

1. Задаются требования по: охране помещений, допуску лиц, выбору технических средств, их расположению в помещениях. Кроме того, задаются дополнительные требования по обеспечению конфиденциальности, целостности и доступности ПДн.

2. К числу мер, необходимых и достаточных для обеспечения выполнения обязанностей оператора относятся:

–Назначение ответственного за организацию обработки ПДн;

–Издание документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

–Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора;

–Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

–Ознакомление работников оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении

обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников;

–Определение угроз безопасности ПДн при их обработке в ИСПДн;

–Применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

–Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

–Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

–Учет машинных носителей ПДн;

–Обнаружение фактов несанкционированного доступа к ПДн и принятие мер;

–Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

–Установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

–Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

3. Обеспечение безопасности ПДн с использованием криптосредств, должно осуществляться в соответствии с:

–Приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);

–Приказом ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" (Зарегистрировано в Минюсте России 18.08.2014 N 33620);

–Настоящими Требованиями.

4. Оператор ПДн несет ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки с использованием криптосредств ПДн, лицензионным требованиям и условиям, эксплуатационной и технической документации к криптосредствам, а также настоящим Требованиям.

5. При этом должна обеспечиваться комплексность защиты ПДн, в том числе посредством применения некриптографических средств защиты.

6. При разработке и реализации мероприятий по организации и обеспечению безопасности ПДн при их обработке в информационной системе осуществляется:

–разработка для каждой ИСПДн модели угроз безопасности ПДн при их обработке;

–разработка на основе модели угроз системы безопасности ПДн, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

–определение необходимости использования криптосредств для обеспечения безопасности ПДн и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн и (или) иных неправомерных действий при их обработке;

–установка и ввод в эксплуатацию средств защиты информации (в том числе криптографических) в соответствии с эксплуатационной и технической документацией к этим средствам;

–проверка готовности средств защиты информации (в том числе криптографических) к использованию с составлением заключений о возможности их эксплуатации;

–поэкземплярный учет используемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

–контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

–разбирательство и составление заключений по фактам нарушения условий хранения носителей ПДн, использования криптосредств, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

–описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности ПДн с использованием криптосредств при их обработке в информационных системах, с указанием в частности:

–индекса, условного наименования и регистрационных номеров, используемых криптосредств;

–соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;

–соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

7. Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

8. Сведения, предусмотренные пунктами 5, 7, 10 и 11 части 3 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» должны быть предоставлены в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

9. Пользователи ИСПДн обязаны:

–не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

–соблюдать требования к обеспечению безопасности ПДн, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

–сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

–немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых ПДн.

–сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

10. Обеспечение функционирования и безопасности ИСПДн возлагается на ответственного пользователя, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь).

11. Ответственные пользователи должны иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

12. При определении обязанностей пользователя необходимо учитывать, что безопасность обработки с использованием криптосредств ПДн обеспечивается:

–соблюдением пользователями криптосредств, конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним;

–точным выполнением пользователями криптосредств, требований к обеспечению безопасности ПДн;

–надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

–обеспечением принятых в соответствии с Требованиями к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн мер.

–своевременным выявлением попыток посторонних лиц получить сведения о защищаемых ПДн, об используемых криптосредствах или ключевых документах к ним;

–немедленным принятием мер по предупреждению разглашения защищаемых ПДн, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

13. Лица, оформляемые на работу в качестве пользователей (ответственных пользователей), должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности ПДн при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

14. В соответствии с требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и установленным уровнем защищенности ПДн, обрабатываемых в ИСПДн «Бухгалтерский и кадровый учет» необходимо выполнение следующих требований:

–контроль за выполнением настоящих Требований организуется и проводится ответственным за организацию обработки, не реже 1 раза в 3 года;

–организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

–обеспечение сохранности носителей ПДн;

–утверждение главным врачом документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

–использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

15. Текущий контроль за организацией и обеспечением функционирования средств защиты информации (в том числе криптографических) возлагается на оператора и ответственного пользователя в пределах их служебных полномочий.

16. Контроль за организацией, обеспечением функционирования и безопасности средств защиты информации (в том числе криптографических), предназначенных для защиты ПДн, при их обработке в ИСПДн осуществляется в соответствии с действующим законодательством Российской Федерации.

17. При использовании в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации, для обеспечения установленного уровня защищенности ПДн применяются:

–средства вычислительной техники не ниже 6 класса;

–системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты;

–межсетевые экраны не ниже 5 класса.

3. Мероприятия по обеспечению безопасности ПДн от несанкционированного доступа при их обработке в ИСПДн

В состав мер по обеспечению безопасности ПДн, реализуемых в рамках СЗПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн (далее - машинные носители ПДн);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности ПДн;
- обеспечение целостности информационной системы и ПДн;
- обеспечение доступности ПДн;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности ПДн (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты ПДн.

В таблице 1 приведено содержание требуемых мер по обеспечению безопасности ПДн:

Таблица 1. Содержание требуемых мер по обеспечению безопасности ПДн

Условное обозначение и номер меры	**Содержание мер по обеспечению безопасности ПДн**
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности ПДн (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования,

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности ПДн
	а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

4. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей

1. Пользователи криптосредств обязаны:

−не разглашать информацию о ключевых документах;

−не допускать снятие копий с ключевых документов;

−не допускать вывод ключевых документов на дисплей (монитор) или принтер;

−не допускать записи на ключевой носитель посторонней информации;

−не допускать установки ключевых документов в другие автоматизированные рабочие места.

2. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3. Криптосредства, используемые для обеспечения безопасности ПДн при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

4. Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

5. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

6. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

7. Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в

соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.

8. Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).

9. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

10. Пользователи криптосредств хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

11. Пользователи криптосредств предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

12. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

13. Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными оператором ответственными пользователями криптосредств и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки.

14. Эксплуатационную и техническую документацию к криптосредствам допускается пересылать заказными или ценными почтовыми отправлениями.

15. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

16. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

17. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также

восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

18. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин.

19. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

20. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная, и хранящаяся в криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

21. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах уничтожаются пользователями этих криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.

22. Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного пользователя криптосредств для списания уничтоженных документов с их лицевых счетов.

23. Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

24. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с оператором, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

25. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием ПДн, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств и (или) оператору.

26. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

27. В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

28. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет оператор.

Приложение № 1 к приказу
ГАУЗ ТО «Городская поликлиника №3»
от «30» декабря 2022 г. № 483-п

Типовая форма

С О Г Л А С И Е
на обработку персональных данных, разрешенных субъектом персональных данных для распространения, в т.ч. для раскрытия неопределенному кругу лиц

Я, _____,
фамилия, имя, отчество полностью
проживающий(ая) по адресу: _____
субъект Российской Федерации, город, улица, дом, корпус, квартира
_____,
паспорт: серия _____ номер _____, выдан _____, дата выдачи _____,
настоящим даю свое согласие *ГАУЗ ТО «Городская поликлиника №3»* ОГРН _1027200828929_ ИНН _7202100346_, зарегистрированной по адресу: 625003, Тюменская обл., г. Тюмень, ул. Ленина, д.23 (далее – Оператор) на обработку моих персональных данных, **разрешенных для распространения, в т.ч. для раскрытия неопределенному кругу лиц,** и подтверждаю, что давая согласие, я действую свободно, по своей воле и в своих интересах.

Мне известны и понятны права, принадлежащие мне как субъекту персональных данных, определенные в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», а также предоставленные Гражданским кодексом Российской Федерации, в части охраны изображения гражданина.

Обработка Оператором моих персональных данных в форме распространения допускается в целях обеспечения соблюдения, применения, исполнения и использования нормативных правовых актов в рамках оказания медицинских услуг.

Я даю согласие в рамках медицинских отношений и иных отношений, связанных с получением медицинских услуг, на распространение:

Таблица 1

Категория персональных данных	Перечень персональных данных	Разрешение к распространению (да/нет)	Условия и запреты
Персональные данные	фамилия		
	имя		
	отчество (при наличии)		
	год рождения		
	месяц рождения		
	дата рождения		
	место рождения		
	адрес		
	семейное положение		
	образование		
	профессия		
	социальное положение		
	доходы		
Специальные категории персональных данных	расовая принадлежность		
	национальность		
	политические взгляды		
	религиозные убеждения		
	философские убеждения		
	состояние здоровья		

	состояние интимной жизни		
	сведения о судимости		
Биометрические персональные данные	ДНК		
	цветное цифровое фото изображение лица		

Сведения об информационных ресурсах оператора, посредством которых будет осуществляться предоставление доступа (раскрытия) неограниченному (неопределенному) кругу лиц и иные действия с персональными данными субъекта персональных данных:

Таблица 2

Информационный ресурс	Действия (ограничения) с персональными данными *(выбрать из перечня ниже; проставить нужную цифру от 1 до 4)*
Официальный сайт *ГАУЗ ТО «Городская поликлиника №3»* https://www.gp3tmn.ru/	

(*нужное выбрать и проставить в Таблицу 2 выше для каждой строки*):

1. не устанавливаю
2. устанавливаю запрет на передачу (кроме предоставления доступа) этих данных оператором неограниченному кругу лиц
3. устанавливаю запрет на обработку (кроме получения доступа) этих данных неограниченным кругом лиц
4. устанавливаю условия обработки (кроме получения доступа) этих данных неограниченным кругом лиц: _____ _____.

Условия и запреты на обработку вышеуказанных персональных данных (ч. 9 ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»)

Условия, при которых полученные персональные данные могут передаваться оператором только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных: *указать нужное*: *не устанавливаю/устанавливаю* _____.

Действия (операции), связанные с обработкой моих персональных данных, разрешенных для распространения, могут производиться с помощью средств вычислительной техники, с использованием информационных технологий, в том числе путем включения в электронные базы данных, используемые Оператором для работы.

Данное согласие может быть отозвано мною в любой момент, но не ранее даты прекращения получения медицинских услуг, с обязательным направлением Оператору письменного уведомления.

С момента получения уведомления об отзыве согласия Оператор обязан прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

Мне известно, что при отзыве мною согласия Оператор вправе: продолжить обработку моих персональных данных в случаях, предусмотренных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», иных нормативных правовых актах; продолжить хранение моих персональных данных, не являющихся биометрическими персональными данными, если обязанность их хранения предусмотрена нормативными правовыми актами, продолжить хранение моего изображения, в том числе, если хранение является обязанностью, которая предусмотрена нормативными правовыми актами.

При достижении целей обработки мои персональные данные могут быть уничтожены в порядке и сроки, установленные в нормативных правовых актах.

Все вышеизложенное мною прочитано, мне понятно и подтверждается собственноручной подписью (подписью законного представителя).

_____ _____ _____

дата подпись инициалы, фамилия

Приложение № 1 к приказу
ГАУЗ ТО «Городская поликлиника №3»
от «30» декабря 2022 г. № 483-п

Типовая форма

СОГЛАШЕНИЕ
О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Я,
_____,
(Ф.И.О.)
Проживающий по адресу:
_____
Паспорт №_____, выданный (кем и когда)
_____
_____
_____

предупрежден(а) о том, что на период исполнения мною должностных обязанностей по Трудовому договору, заключенному между мною и *ГАУЗ ТО «Городская поликлиника №3»*, и предусматривающих работу с персональным данными, мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:

– не передавать (в любом виде) и не разглашать третьим лицам и работникам *ГАУЗ ТО «Городская поликлиника №3»*, не имеющим на это право, информацию, содержащую персональные данные (за исключением собственных данных), которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

– в случае попытки третьих лиц или работников *ГАУЗ ТО «Городская поликлиника №3»*, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному руководителю;

– не использовать информацию, содержащую персональные данные, с целью получения выгоды;

– выполнять требования законодательства Российской Федерации, а также внутренних документов *ГАУЗ ТО «Городская поликлиника №3»*, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

Я ознакомлен(а) с положениями законодательства Российской Федерации, а также внутренними организационно-распорядительными документами *ГАУЗ ТО «Городская поликлиника №3»*, в части защиты персональных данных.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

_____/_____ «___» _____ _____ г.
(фамилия, инициалы) (подпись)