РОССИЙСКАЯ ФЕДЕРАЦИЯ
ХАНТЫ-МАНСИЙСКИЙ АВТОНОМНЫЙ ОКРУГ-ЮГРА
ГОРОД ОКРУЖНОГО ЗНАЧЕНИЯ СУРГУТ

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «МЕДИЦИНСКИЙ ЦЕНТР НАИРИ МЕД» (ООО «МЦ НАИРИ МЕД»)

628407, Ханты-Мансийский Автономный Округ - Югра, г.о. Сургут, г. Сургут, ул. Семена Билецкого, д. 6, помещ. этаж 1
ОГРН 1228600003158, ИНН 8602306022, КПП 860201001

Утверждаю
Генеральный директор ООО «МЦ НАИРИ МЕД»
Т.О. Мнацаканян _____
«01» января 2026 года

ПОЛОЖЕНИЕ О ЗАЩИТЕ, ХРАНЕНИИ, ОБРАБОТКЕ И ПЕРЕДАЧЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рег.№ ПДн-1

г. Сургут
2026 год

Введение.

Настоящее Положение о защите, хранении, обработке и передаче персональных данных (далее – Положение) разработано с целью систематизации в Обществе с ограниченной ответственностью «Медицинский центр Наири Мед» (далее – ООО «МЦ НАИРИ МЕД», Организация) подхода к защите, хранению, обработке и передаче таких сведений внутри компании, учитывая специфику медицинской деятельности.

Внедрение единых правил помогает не только минимизировать риски утечек и несанкционированного доступа, но и выстроить прозрачную систему ответственности для всех сотрудников, задействованных в работе с информацией.

Положение ориентировано на практическое применение: в нем описаны конкретные механизмы взаимодействия между подразделениями, порядок получения согласий, правила передачи данных третьим лицам и меры по обеспечению безопасности при использовании информационных систем.

Настоящее Положение о защите, хранении, обработке и передаче персональных данных (далее – Положение) регламентируется:

– Конституцией Российской Федерации;

– Трудовым кодексом Российской Федерации;

– Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

– Федеральным законом от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";

– Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных"

– и иными нормативными правовыми актами в области обработки и защиты персональных данных.

Организация является оператором персональных данных и осуществляет обработку персональных данных в соответствии с законодательством Российской Федерации.

Действие настоящего Положения распространяется на всех сотрудников ООО «МЦ НАИРИ МЕД», а также лиц, осуществляющих обработку и использование персональных данных на основании договора оказания услуг (бухгалтерских, аудиторских и т.п.).

Перечень сотрудников, допущенных к обработке персональных данных указан в Приложении №1 к настоящему Положению.

Ознакомление работников с настоящим Положением осуществляется при приеме на работу (до подписания трудового договора). Факт ознакомления работника подтверждается подписью в листе ознакомления, являющемся неотъемлемой частью настоящего Положения.

Настоящее Положение вступает в силу с даты его утверждения Генеральным директором ООО «МЦ НАИРИ МЕД».

Положение пересматривается при изменении законодательства о персональных данных, изменении организационной структуры Организации или применяемых информационных систем.

Изменения в настоящее Положение вносятся приказом Генерального директора. Все работники уведомляются об изменениях под роспись.

По всем вопросам, не урегулированным настоящим Положением, Организация руководствуется действующим законодательством Российской Федерации.

Предоставление копии или выдержек из инструкции допускается исключительно на основании письменного разрешения генерального директора и при условии подписания соглашения о неразглашении информации; иным лицам — только с письменного согласия высшего органа управления организации.

1. Общие положения о защите персональных данных.

1.1. В настоящем Положении используются следующие основные понятия:

Персональные данные — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Субъект персональных данных — физическое лицо, чьи персональные данные обрабатываются Оператором.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

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

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

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

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

Специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Оператор персональных данных — ООО «МЦ НАИРИ МЕД», самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных.

МИС — Медицинская информационная система, используемая Организацией для учёта пациентов и медицинской документации.

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным лицом требование не допускать распространения персональных данных без согласия субъекта.

2. Категории персональных данных, обрабатываемых в организации. Цели обработки персональных данных.

2.1. В ООО «МЦ НАИРИ МЕД» обрабатывает следующие персональные данные:

№ п/п	Категория субъекта персональных данных	Категория персональных данных	Перечень персональных данных

1	Сотрудники (лица, заключившие трудовой договор с ООО «МЦ НАИРИ МЕД», в том числе те лица, которые ранее состояли в трудовых отношениях с ООО «МЦ НАИРИ МЕД»)	Иные Специальные	- фамилия, имя, отчество (в том числе предыдущие фамилии, имена, отчества в случае их изменения); - число, месяц, год рождения; - место рождения; - пол; - гражданство; - место жительства (в том числе сведения о регистрации по месту жительства / месту пребывания); - данные документы удостоверяющего личность (серия, номер, дата выдачи, наименование и код подразделения органа, выдавшего документ; - место работы, профессия (специальность); - сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); - сведения об образовании и повышении квалификации; - сведения о воинском учете; - ИНН; - СНИЛС; - сведения о доходах; - информация по лицевому банковскому счету сотрудника; - результаты обязательных медицинских осмотров; - сведения о контактных данных (номер телефона, адрес электронной почты); - иные персональные данные, учитываемые в формах статистического и медико-статистического наблюдения и информационных системах органов управления здравоохранением федерального и территориального уровней.
2	Кандидаты (соискатели) на замещение вакантных должностей ООО «МЦ НАИРИ МЕД»	Иные Специальные	- фамилия, имя, отчество (в том числе предыдущие фамилии, имена, отчества в случае их изменения); - число, месяц, год рождения; - место рождения; - пол; - гражданство; - место работы, профессия (специальность); - сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации); - сведения об образовании и повышении квалификации; - сведения о контактных данных (номер телефона, адрес электронной почты).
3	Пациенты (лица, обратившиеся за медицинской упомощью в ООО «МЦ НАИРИ МЕД»)	Иные Специальные	- фамилия, имя, отчество (в том числе предыдущие фамилии, имена, отчества в случае их изменения); - число, месяц, год рождения; - пол; - гражданство; - место жительства (в том числе сведения о регистрации по месту жительства / месту пребывания);

			- данные документы удостоверяющего личность (серия, номер, дата выдачи, наименование и код подразделения органа, выдавшего документ; - место работы, профессия (специальность); - ИНН; - СНИЛС; - сведения о контактных данных (номер телефона, адрес электронной почты); - данные полиса добровольного медицинского страхования; - сведения о законном представителе (при наличии); - анамнез; - диагноз; - данные лабораторных исследований; - диагноз заболевания (состояния); - вид оказанной медицинской помощи; - условия оказанной медицинской помощи, включая сведения о сроках, объеме и результатах оказанных медицинских услуг; - примененные стандартны медицинской помощи; - сведения о медицинском работниках, оказавших медицинскую услугу; - аудио- и видеозаписи из помещений медицинского центра, оборудованных устройствами аудио- и видео- фиксации.
4	Родители или законные представители пациентов	Иные	- фамилия, имя, отчество (в том числе предыдущие фамилии, имена, отчества в случае их изменения); - число, месяц, год рождения; - пол; - гражданство; - место жительства (в том числе сведения о регистрации по месту жительства / месту пребывания); - данные документы удостоверяющего личность (серия, номер, дата выдачи, наименование и код подразделения органа, выдавшего документ; - место работы, профессия (специальность); - ИНН; - СНИЛС; - сведения о контактных данных (номер телефона, адрес электронной почты); - данные полиса добровольного медицинского страхования; - семейный анамнез; - аудио- и видеозаписи из помещений медицинского центра, оборудованных устройствами аудио- и видео- фиксации.
5	Контрагенты, их работники и представители	Иные	- фамилия, имя, отчество (в том числе предыдущие фамилии, имена, отчества в случае их изменения); - число, месяц, год рождения; - пол; - данные документы удостоверяющего личность (серия, номер, дата выдачи, наименование и код подразделения органа, выдавшего документ; - место работы, профессия (специальность); - сведения о контактных данных (номер телефона, адрес электронной почты).

6	Посетители сайта ООО «МЦ НАИРИ МЕД»	Иные	- фамилия, имя, отчество; - число, месяц, год рождения; - пол; - сведения о контактных данных (номер телефона, адрес электронной почты).

2.2. Обработка персональных данных ООО «МЦ НАИРИ МЕД» ограничивается достижением следующих целей:

2.2.1. Цели обработки персональных данных сотрудников:

– ведение кадрового и бухгалтерского учета в соответствии с законодательством Российской Федерации;

– обеспечение соблюдения трудового законодательства Российской Федерации;

– обеспечение соблюдения налогового законодательства Российской Федерации;

– обеспечение соблюдения пенсионного законодательства Российской Федерации;

– обеспечение соблюдения страхового законодательства Российской Федерации;

– предоставление сведений в банковские организации для перечисления заработной платы и иных выплат;

– информирование граждан о деятельности ООО «МЦ НАИРИ МЕД»;

– проведение рекламных кампаний ООО «МЦ НАИРИ МЕД»;

2.2.2. Цели обработки персональных данных уволенных сотрудников:

– ведение кадрового и бухгалтерского учета в соответствии с законодательством Российской Федерации;

– обеспечение соблюдения трудового законодательства Российской Федерации;

обеспечение соблюдения налогового законодательства Российской Федерации.

2.2.3. Цели обработки персональных данных лиц, обращающихся в ООО «МЦ НАИРИ МЕД» за оказанием медицинской помощи, а также их законных представителей:

– заключение и исполнение договора оказания медицинских услуг;

– обеспечение соблюдения законодательства Российской Федерации в сфере здравоохранения;

– обеспечение соблюдения налогового законодательства Российской Федерации;

– ведение бухгалтерского учета в соответствии с законодательством Российской Федерации;

– проведение внутреннего контроля качества оказания медицинских услуг;

– информирование граждан о деятельности ООО «МЦ НАИРИ МЕД»;

– проведение рекламных кампаний ООО «МЦ НАИРИ МЕД».

2.2.4. Цели обработки персональных данных контрагентов, их работников или представителей:

– исполнение договорных обязательств ООО «МЦ НАИРИ МЕД».

2.2.5. Цели обработки персональных данных посетителей сайта ООО «МЦ НАИРИ МЕД»:

– осуществление обратной связи, включая направление уведомлений, запросов, касающихся оказание услуг, обработки запросов и заявок от посетителей сайта;

– проведение статистических и иных исследований по работе сайта на основе обезличенных персональных данных посетителей сайта.

2.3. ООО «МЦ НАИРИ МЕД» не обрабатывает персональные данные, которые не совместимы с целями обработки персональных данных.

3. Принципы обработки персональных данных.

3.1. Обработка персональных данных в Организации осуществляется на основе следующих принципов:

3.1.1. Законность и справедливость. Обработка ПД осуществляется исключительно на законных основаниях, установленных статьёй 6 и статьёй 10 Федерального закона № 152-ФЗ.

3.1.2. Ограничение цели. Обработка ПД осуществляется только в заранее определённых, чётко сформулированных и законных целях. Не допускается обработка ПД в целях, несовместимых с целями их сбора.

3.1.3. Минимизация данных. Обрабатываются только те ПД, которые необходимы для достижения конкретных заявленных целей.

3.1.4. Точность данных. Принимаются все разумные меры для обеспечения актуальности и достоверности обрабатываемых ПД.

3.1.5. Ограничение хранения. ПД хранятся не дольше, чем это необходимо для достижения цели их обработки.

3.1.6. Целостность и конфиденциальность. Применяются надлежащие технические и организационные меры для защиты ПД от несанкционированного или незаконного доступа, случайной утраты, уничтожения или повреждения.

3.1.7. Подотчётность. Организация несёт ответственность за соблюдение всех перечисленных принципов и способна продемонстрировать их соблюдение.

4. Условия и порядок сбора персональных данных.

4.1. Сбор персональных данных пациентов осуществляется:

– при первичном обращении пациента в регистратуру путём заполнения анкеты/карты пациента;

– при заключении договора на оказание медицинских услуг;

– в процессе оказания медицинской помощи.

4.2. Сбор персональных данных работников осуществляется:

– при приёме на работу путём представления документов, предусмотренных статьёй 65 ТК РФ;

– в процессе трудовой деятельности.

4.3. До начала обработки персональных данных Организация обязана:

– получить письменное согласие субъекта персональных данных на обработку его ПД (за исключением случаев, предусмотренных законом);

– ознакомить субъекта с Политикой в отношении обработки персональных данных;

– разъяснить субъекту его права.

4.4. Согласие на обработку персональных данных, в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» должно:

– быть конкретным, информированным, сознательным и однозначным;

– оформляться в допустимой законом форме (в т.ч. электронной);

– включать обязательные сведения (цели, перечень данных, срок действия и др.);

– предусматривать право субъекта на отзыв.

4.5. Согласие на обработку персональных данных оформляется отдельным документом, по формам, представленным в Приложении №2, 3, 4. Согласие на обработку персональных данных не включается в состав иных документов.

Согласие субъекта персональных данных на обработку его персональных данных предоставляется в письменной форме (в том числе в виде электронного документа, подписанного электронной подписью) или иным способом, предусмотренным законодательством РФ.

В письменной форме (включая электронную) согласия содержаться следующие данные (ч. 4 ст. 9 ФЗ № 152-ФЗ):

– ФИО, адрес, данные документа, удостоверяющего личность субъекта;

– данные представителя субъекта (если согласие даётся через представителя), включая реквизиты доверенности;

– наименование и адрес оператора;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых даётся согласие;

– наименование и адрес лица, осуществляющего обработку по поручению оператора (если применимо);

– перечень действий с данными и способы их обработки;

– срок действия согласия и способ его отзыва;

– подпись субъекта (или электронная подпись в электронном документе).

4.6. Сбор ПД без согласия субъекта допускается в случаях, предусмотренных федеральным законодательством (оказание экстренной медицинской помощи, исполнение требований законодательства и др.).

4.7. Согласие на обработку персональных данных может быть отозвано субъектом в любой момент путём направления письменного заявления Оператору.

4.8. В случае отзыва согласия Оператор прекращает обработку персональных данных, за исключением случаев, когда обработка допускается без согласия субъекта в соответствии с законодательством РФ.

5. Организационные и технические меры, предпринимаемые в ходе обработки персональных данных.

5.1. Организационные меры в сфере обработки персональных данных.

5.1.1. Для организации работы с персональными данными в Организации назначается Ответственный за организацию обработки персональных данных (далее — Ответственный) приказом Генерального директора.

5.1.2. Ответственный выполняет следующие функции:

– осуществляет внутренний контроль за соблюдением законодательства о персональных данных;

– доводит до сведения работников положения законодательства о ПД и настоящего Положения;

– организует приём и обработку обращений субъектов ПД;

– взаимодействует с Роскомнадзором;

– обеспечивает актуальность локальных нормативных актов по защите ПД;

– организует обучение сотрудников.

5.1.3. Перечень сотрудников, имеющих доступ к персональным данным, формируется на основании их должностных обязанностей и утверждается приказом Генерального директора. Перечень пересматривается не реже одного раза в год, а также при изменении штатного расписания.

5.1.4. Каждый сотрудник, включённый в Перечень, подписывает Соглашение о неразглашении персональных данных и несёт дисциплинарную, административную и уголовную ответственность за нарушение режима конфиденциальности.

5.1.5. Инструктаж по вопросам работы с персональными данными проводится:

– при приёме на работу (первичный инструктаж);

– не реже одного раза в год (плановый инструктаж);

– при изменении нормативно-правовой базы (внеплановый инструктаж).

5.1.6. В Организации ведётся Журнал учёта инструктажей по защите персональных данных с указанием даты, темы, ФИО проводившего инструктаж и подписей прошедших его сотрудников.

5.2. Технические меры защиты (продолжение)

5.2.1. Все рабочие места, на которых осуществляется обработка персональных данных, оснащаются:

– лицензионным антивирусным программным обеспечением с актуальными базами обновлений;

– межсетевыми экранами (программными или аппаратными);

– средствами разграничения доступа (парольная аутентификация, при необходимости — двухфакторная аутентификация).

5.2.2. Требования к паролям:

– длина не менее 8 символов;

– обязательное использование букв верхнего и нижнего регистра, цифр, специальных символов;

– смена пароля не реже одного раза в 90 дней;

– запрет повторного использования последних 5 паролей;

– блокировка учётной записи после 5 неудачных попыток ввода пароля.

5.2.3. Автоматическая блокировка экрана рабочего места устанавливается при отсутствии активности пользователя более 10 минут.

5.2.4. Использование съёмных носителей информации (USB-накопители, внешние жёсткие диски) допускается только с разрешения Ответственного и только для служебных целей.

5.2.5. Передача персональных данных по электронным каналам связи осуществляется исключительно с использованием защищённых каналов.

5.2.6. Серверное оборудование размещается в специально отведённом помещении (серверной комнате), доступ в которое ограничен и осуществляется только уполномоченными лицами или осуществляется у сторонней организации, занимающейся информационным сопровождением деятельности Организации.

5.2.7. Резервное копирование данных осуществляется ежедневно в автоматическом режиме. Резервные копии хранятся в защищённом месте, географически удалённом от основного сервера, либо в защищённом облачном хранилище.

5.2.8. Обновление операционных систем, прикладного программного обеспечения и антивирусных баз осуществляется регулярно, не реже одного раза в месяц.

6. Регламент работы с персональными данными.

6.1. Обработка персональных данных осуществляется при наличии хотя бы одного из следующих оснований:

– согласие субъекта персональных данных;

– обработка необходима для исполнения договора, стороной которого является субъект ПД;

– обработка необходима для исполнения обязанностей, возложенных на Организацию законодательством РФ;

– обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД;

– обработка осуществляется в медицинских целях при условии соблюдения врачебной тайны медицинскими работниками.

6.2. Документы, содержащие персональные данные, создаются путем:

– копирования оригиналов;

– внесения сведений в учетные формы (на бумажных и электронных носителях);

– получения оригиналов необходимых документов.

6.3. Обработка персональных данных в ООО «МЦ НАИРИ МЕД» осуществляется следующими способами:

– неавтоматизированная обработка персональных данных;

– автоматизированная обработка персональных данных;

– смешанная обработка персональных данных.

6.4. Все персональные данные субъекта получаются у него самого или у его законного представителя, за исключением случаев, если их получение возможно только у третей стороны.

6.5. ООО «МЦ НАИРИ МЕД» совершает с персональными данными субъектов следующие действия:

– сбор;
– запись;
– систематизация;
– накопление;
– хранение;
– уточнение (обновление, изменение);
– извлечение;
– использование;
– передача (распространение, предоставление, доступ);
– обезличивание;
– блокирование;
– удаление;
– уничтожение.

6.6. ООО «МЦ НАИРИ МЕД» не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях в частной жизни, за исключением случаев, предусмотренных законодательством.

6.7. ООО «МЦ НАИРИ МЕД» не осуществляет обработку биометрических персональных данных.

6.8. ООО «МЦ НАИРИ МЕД» осуществляет обработку специальных категорий персональных данных в части информации, касающейся состояния здоровья субъекта персональных данных.

Обработка специальных категорий персональных данных производится в целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных.

6.9. Сроки обработки персональных данных определяются в соответствии со сроком действия договора (трудового / гражданского-правового) с субъектом персональных данных, а также с требованиями законодательства Российской Федерации и нормативными документами, регламентирующими сроки хранения и обработки такой информации.

Обработка персональных данных прекращается при отзыве субъектом согласия на обработку своих персональных данных, за исключением случаев, предусмотренных в пунктах 2-11 части 1 статьи 6 и части 2 статьи 10 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

6.10. Регламент работы с персональными данными в МИС.

6.10.1. Медицинская информационная система (МИС) является основной ИСПДн Организации, в которой хранятся и обрабатываются персональные данные пациентов.

В МИС организуется разделение пользователей со следующими правами доступа:

Роль	Доступные модули	Чьи персональные данные содержаться в доступных модулях
Администратор	Управление пользователями	Сотрудники ООО «МЦ НАИРИ МЕД»
Врач	Медицинские карты пациентов	Пациенты Сотрудники ООО «МЦ НАИРИ МЕД»
Средний медперсонал	Лаборатория Медицинские карты пациентов	Пациенты Сотрудники ООО «МЦ НАИРИ МЕД»
Регистратура (администратор)	Расписание приема врачей Лаборатория Медицинские карты	Пациенты Сотрудники ООО «МЦ НАИРИ МЕД»

	Касса Отчетность	
Бухгалтерия	Касса Отчетность	Пациенты (без доступа к медицинским записям) Сотрудники ООО «МЦ НАИРИ МЕД»
Главный врач и его заместителя	Полный доступ в систему	Пациенты Сотрудники ООО «МЦ НАИРИ МЕД»
Генеральный директор	Полный доступ в систему	Пациенты Сотрудники ООО «МЦ НАИРИ МЕД»

6.10.2. Каждому пользователю МИС присваивается уникальный логин и персональный пароль.

Передача учётных данных третьим лицам категорически запрещена.

При увольнении сотрудника его учётная запись в МИС блокируется в день увольнения (не позднее).

6.10.3. Все действия пользователей фиксируются в журнале аудита МИС (лог-файлах) с указанием логина, даты, времени и характера действия.

Лог-файлы хранятся не менее 1 года и проверяются Ответственным не реже одного раза в квартал.

6.10.4. Внесение данных в МИС осуществляется в соответствии с утверждёнными инструкциями по работе с системой.

6.10.5. Не допускается:

– вносить в МИС заведомо недостоверную информацию;

– удалять записи без соответствующего приказа и акта;

– использовать учётные данные других пользователей;

– копировать данные из МИС на внешние носители без разрешения ответственного лица.

6.10.6. При обнаружении ошибок в данных МИС пользователь обязан незамедлительно сообщить об этом администратору системы для исправления.

6.10.7. Передача данных из МИС осуществляется в соответствии с разделом 8 настоящего Положения.

6.10.8. Выгрузка данных из МИС в любых форматах допускается исключительно в целях исполнения трудовых функций.

6.10.9. Персональные данные пациентов вносятся в МИС при первичном обращении за оказанием медицинской помощи в соответствии с Инструкцией о работе в МИС.

Персональные данные пациентов, указанные в разделе 2 настоящего Положения, включаются в состав следующих документов, формируемых в МИС:

– согласие на обработку персональных данных;

– медицинская карта пациента получающего медицинскую помощь в амбулаторных условиях;

– договор на оказание платных медицинских услуг;

– спецификация к договору оказания платных медицинских услуг;

– информированное добровольное согласие на оказание медицинской помощи;

– акт оказанных услуг;

– заключение врача;

– направление на лабораторные исследования (заказ в лабораторию);

– квитанция об оплате медицинских услуг / справка об оплате медицинских услуг.

6.10.10. Согласие на обработку персональных данных формируется в МИС при первичном обращении пациента.

Согласие оформляется в виде отдельного документа в соответствии с разделом 4 настоящего Положения.

Согласие храниться вшитым в медицинскую карту пациента.

6.10.11. Медицинская карта пациента создаётся при первичном обращении и ведётся в МИС в электронном виде с дублированием на бумажном носителе.

Все записи в медицинской карте подписываются электронной подписью врача либо заверяются собственноручной подписью.

Исправления в записях допускаются только путём добавления новой записи с указанием причины исправления. Удаление ранее внесённых записей запрещено.

6.10.11. Договор на оказание платных медицинских услуг и спецификации к нему формируется в виде отдельного документа и храниться в составе медицинской карты пациента.

6.10.12. Результаты лабораторных и инструментальных исследований вносятся в МИС в день их получения.

6.10.13. При выдаче пациенту на руки каких-либо медицинских документов (выписки, справки, заключения) факт выдачи документов учитывается в МИС или журнале выдачи документации с указанием даты и ФИО получателя.

6.11. Регламент работы с персональными данными в 1С

6.11.1. В программном комплексе «1С:Предприятие» (конфигурации «1С:Бухгалтерия» и «1С:Зарплата и управление персоналом») обрабатываются:

– персональные данные работников для целей кадрового учёта, расчёта и выплаты заработной платы, формирования отчётности;

– персональные данные пациентов в части финансовых взаиморасчётов (реквизиты договоров,.фискальные документы, акты).

6.11.2. Каждому пользователю 1С присваивается уникальная учётная запись.

Передача логина и пароля другим лицам запрещена.

6.11.3. После завершения работы в 1С сотрудник обязан завершить сеанс (выйти из системы).

6.11.4. Выгрузка данных из 1С в файлы (Excel, CSV и др.) допускается только для служебных целей.

Все отчёты, содержащие персональные данные, распечатанные на бумажном носителе, учитываются и хранятся в соответствии с разделом 7 настоящего Положения.

6.11.5. Отчётность в государственные органы Российской Федерации передается в соответствии с разделом 8 настоящего Положения.

6.12. Обработка ПД осуществляется уполномоченными сотрудниками Организации в пределах, установленных их должностными инструкциями и настоящим Положением.

6.13. Каждый сотрудник, получивший доступ к ПД, несёт персональную ответственность за их сохранность и конфиденциальность.

6.14. Обработка ПД с использованием средств автоматизации и без таковых осуществляется с соблюдением требований ФЗ № 152-ФЗ.

6.15. Не допускается раскрытие третьим лицам и распространение ПД без согласия субъекта, если иное не предусмотрено законодательством.

7. Хранение персональных данных.

7.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом или договором, стороной которого является субъект персональных данных.

7.2. Персональные данные хранятся:

– в информационных системах с применением средств защиты информации;

– на бумажных носителях в запираемых шкафах/сейфах, в помещениях с ограниченным доступом.

7.3. Доступ к персональным данным имеют только уполномоченные сотрудники Оператора, которым это необходимо для выполнения трудовых обязанностей.

7.4. Сроки хранения персональных данных определяются:

– требованиями федеральных законов (в т. ч. ФЗ «О персональных данных»);

– условиями договоров с субъектами персональных данных;

– внутренними регламентами ООО «МЦ НАИРИ МЕД».

7.5. По истечении срока хранения или достижении целей обработки персональные данные подлежат уничтожению или обезличиванию.

7.6. В ООО «МЦ НАИРИ МЕД» обрабатывает и хранит документы, содержащие персональные данные в следующие сроки:

№ п/п	Категория субъекта персональных данных	Цель обработки	Срок обработки	Срок хранения
1	Сотрудники (лица, заключившие трудовой договор с ООО «МЦ НАИРИ МЕД», в том числе те лица, которые ранее состояли в трудовых отношениях с ООО «МЦ НАИРИ МЕД»)	- ведение кадрового и бухгалтерского учёта в соответствии с законодательством РФ; - обеспечение соблюдения трудового, налогового, пенсионного и страхового законодательства РФ; - предоставление сведений в банковские организации для перечисления заработной платы и иных выплат; - информирование о деятельности медицинского центра; - проведение рекламных кампаний медицинского центра.	Обработка осуществляется с даты подписания трудового договор на весь срок действия трудового договора.	Максимальный срок хранения : 50 лет с даты прекращения трудового договора.
2	Кандидаты (соискатели) на замещение вакантных должностей ООО «МЦ НАИРИ МЕД»	- оценка соответствия соискателя вакантной должности; - оформления трудовых отношений в случае приёма на работу.	Обработка осуществляется с даты подписания согласия на обработку персональных данных до принятия решения о трудоустройстве / отказе в трудоустройстве соискателя, но не более 60 календарных дней с момента получения согласия на обработку персональных данных.	Хранение осуществляется в течение 30 календарных дней после принятия решения о трудоустройстве/отказе в трудоустройстве соискателя.
3	Пациенты (лица, обратившиеся за медицинской помощью в ООО «МЦ НАИРИ МЕД»)	- заключение и исполнение договора оказания медицинских услуг; - обеспечение соблюдения законодательства РФ в сфере здравоохранения;	Обработка осуществляется с даты подписания согласия на обработку персональных данных и в течение 25 лет	Максимальный срок хранения: 50 лет с момента последнего обращения пациента за

	Родители или законные представители пациентов	- обеспечение соблюдения налогового законодательства РФ; - ведение бухгалтерского учёта в соответствии с законодательством РФ; - проведение внутреннего контроля качества оказания медицинских услуг; - информирование о деятельности медицинского центра; - проведение рекламных кампаний медицинского центра; - соблюдение требований о врачебной тайне и иных норм, регулирующих обращение с медицинскими данными; - обработка медицинских данных исключительно в целях оказания медицинской помощи, проведения исследований, статистического учёта и иных целей, предусмотренных законодательством в сфере охраны здоровья.	после последнего обращения пациента за оказанием медицинской помощи.	оказанием медицинской помощи.
4	Контрагенты, их работники и представители	-исполнение договорных обязательств; - обеспечение взаимодействия по договорам; - учёт контрагентов.	Обработка осуществляется с момента заключения договора в течение срока его действия.	Хранение осуществляется в течение 5 лет с момента окончания договора.
5	Посетители сайта ООО «МЦ НАИРИ МЕД»	- предоставления запрашиваемых услуг или информации через сайт; - анализ пользовательского поведения и улучшения функционала сайта; - коммуникации с посетителем; - в иных целях, на которые посетитель дал согласие (например, рассылка новостей, предложений).	Обработка осуществляется до достижения целей обработки персональных данных.	Срок хранения персональных данных, позволяющих идентифицировать посетителя сайта составляет 30 календарных дней с момента получения согласия на обработку персональных данных. Срок хранения обезличенных персональных данных составляет 2 года.

7.7. Бумажный архив документов, содержащих персональные данные, формируется в Организации в целях обеспечения сохранности документации, соблюдения установленных сроков хранения и обеспечения возможности использования документов в законных целях.

7.8. Ответственность за формирование, ведение и хранение бумажного архива возлагается на:

– по документам пациентов — уполномоченного сотрудника регистратуры;

– по кадровым документам — специалиста по кадрам;

– по бухгалтерским документам — главного бухгалтера.

7.9. Помещение, в котором хранится бумажный архив, должно отвечать следующим требованиям:

– наличие металлических стеллажей или шкафов с замками;

– ограниченный доступ: только уполномоченные сотрудники;

– наличие замка на двери помещения, ключи хранятся у ответственного лица;

– соблюдение требований противопожарной безопасности (наличие огнетушителя, исправной проводки);

– соблюдение температурно-влажностного режима (температура 17–19°C, влажность 50–55%);

– отсутствие прямого солнечного света на документы.

7.10. Документы в бумажном архиве группируются по следующим признакам:

– категория субъекта ПД (пациенты / работники / контрагенты);

– вид документа (медицинские карты / согласия / трудовые договоры / кадровые приказы / бухгалтерские документы);

– хронологический период (год, квартал).

7.11. Каждое дело (папка) оформляется в соответствии со следующими требованиями:

– на титульном листе указываются: наименование Организации, наименование дела, период хранящихся документов, дата формирования дела, срок хранения, ФИО ответственного;

– документы внутри дела располагаются в хронологическом порядке;

– листы дела нумеруются карандашом в правом верхнем углу;

– к каждому делу составляется внутренняя опись с перечнем вложенных документов.

Дела формируются на основании номенклатуры дел, утвержденной в Организации.

7.12. Оригиналы документов, содержащих специальные категории персональных данных (сведения о здоровье), не могут быть выданы на руки субъекту ПД — выдаются только заверенные копии. Исключения устанавливаются законодательством.

7.13. Медицинские карты пациентов, обращавшихся в течение текущего и предыдущего года, хранятся в регистратуре в закрытых картотечных шкафах, упорядоченных в алфавитном или нумерационном порядке по системе, установленной Организацией.

Карты пациентов, не обращавшихся более 1 года, передаются в бумажный архив.

Медицинские карты несовершеннолетних хранятся в отдельном разделе с соответствующей маркировкой.

Доступ к медицинским картам в регистратуре разрешён только сотрудникам, включённым в утверждённый Перечень. Оставлять медицинские карты в доступном для посторонних лиц месте запрещено.

Выдача медицинской карты пациенту на руки не производится. По запросу пациента выдаётся заверенная выписка или копия медицинской карты в установленном законом порядке.

7.14. Подписанные пациентами согласия на обработку персональных данных хранятся в медицинских картах пациентов (согласи пациентов) и в отдельной папке (согласия работников)

Электронные копии согласий хранятся в МИС (для пациентов) и в 1С (для работников) с привязкой к карточке соответствующего субъекта.

7.15. Ответственный за архив обязан:

– ежеквартально проводить визуальный осмотр состояния документов;

– незамедлительно докладывать руководству о случаях порчи, утраты или несанкционированного доступа к документам;

– обеспечивать соблюдение температурно-влажностного режима в помещении архива.

При обнаружении утраты или порчи документов составляется акт с указанием обстоятельств и объёма утраченных/повреждённых данных. Ответственный информирует Генерального директора и Ответственного за обработку ПД.

7.16. Подробный порядок оперативного и архивного хранения документов утверждается отдельным Положением/Инструкцией.

8. Передача персональных данных.

8.1. Передача персональных данных субъектов осуществляется ООО «МЦ НАИРИ МЕД» в строгом соответствии с требованиями нормативных правовых актов.

8.2. Передача персональных данных третьим лицам допускается исключительно в случаях, предусмотренных действующим законодательством, на основании договора, содержащего обязательства получателя по обеспечению конфиденциальности и безопасности передаваемых данных, либо на основании письменного согласия субъекта персональных данных.

8.3. Организация передает только тот объём персональных данных, который необходим для достижения конкретной, заранее определённой цели.

8.4. Передача персональных данных в личный кабинет пациента (связанное приложение с МИС, используемой в организации) осуществляется с целью предоставления доступа к медицинским данным для информирования о результатах обследований, записи на приём, получения медицинских документов в электронном виде.

8.5. В личном кабинете пациента содержаться все медицинские документы, сформированные ООО «МЦ НАИРИ МЕД» в ходе оказания медицинской помощи.

Все документы, передаваемые в личный кабинет пациента, содержат те же персональные данные, что и документы в МИС Организации.

8.6. Передача осуществляется на основании согласия пациента на обработку персональных данных, выраженного при регистрации в личном кабинете.

8.7. Доступ к личному кабинету обеспечивается посредством аутентификации по номеру телефона, зарегистрированном в МИС как контактном телефоне пациента. Доступ к сведениям, составляющим врачебную тайну, предоставляется исключительно самому пациенту либо его законному представителю при подтверждении полномочий в установленном порядке.

8.8. Передача персональных данных подрядным организациям осуществляется в целях:

– проведения лабораторных и инструментальных исследований, которые выполняются сторонними лабораториями по договору;

– ведения бухгалтерского учёта, подготовки первичной учётной документации и налоговой отчётности;

– оказания иных услуг, необходимых для деятельности Медицинского центра (IT-обслуживание, юридическое сопровождение, страховые организации и пр.).

8.9. Объём передаваемых персональных данных определяется исходя из цели передачи:

Получатель	Передаваемые Персональных данных
Сторонняя лаборатория	ФИО, дата рождения, пол, номер направления, клинический диагноз, биоматериал и его маркировка
Бухгалтерия / аутсорсинг	ФИО пациента, реквизиты договора, сведения об оказанных услугах и их стоимости
IT-подрядчик	Доступ к Персональных данных предоставляется только в объёме, необходимом для технического обслуживания, под контролем сотрудников Оператора

8.10. Передача персональных данных осуществляется на основании согласия пациента на передачу данных третьим лицам, а также требований законодательства в части ведения бухгалтерского учёта.

8.11. Подрядная организация в обязательном порядке соблюдает конфиденциальность и безопасности персональных данных, не передает их другим лицам, за исключением определенных обстоятельств, определенных в законе Российской Федерации. Обязательства подрядной организации устанавливаются в договоре на оказание конкретных услуг.

8.12. Передача персональных данных в Единую государственную информационную систему в сфере здравоохранения осуществляется в целях исполнения Организацией обязанностей, установленных Федеральным законом от 29.07.2017 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» и Приказом Минздрава России от 07.09.2020 № 947н.

8.13. В ЕГИСЗ передаются следующие сведения:

– идентификационные данные пациента (ФИО, дата рождения, СНИЛС, полис ОМС, паспортные данные);

– сведения о медицинских документах: электронные медицинские документы (ЭМД), в том числе протоколы осмотров, выписные эпикризы, направления, рецепты;

– сведения о случаях оказания медицинской помощи;

– данные о прививках и профилактических мероприятиях (при наличии).

8.14. Интеграция МИС Организации с ЕГИСЗ осуществляется посредством защищённых каналов связи с использованием СКЗИ, сертифицированных ФСБ России. Передача данных осуществляется через региональный сегмент ЕГИСЗ (РИСЗ) с применением усиленной квалифицированной электронной подписи (УКЭП) медицинских работников. Организация обеспечивает актуальность и достоверность передаваемых сведений.

8.15. Выгрузка данных из МИС в систему «1С:Бухгалтерия» осуществляется в целях ведения бухгалтерского и налогового учёта, формирования первичной учётной документации, подготовки счетов на оплату, актов об оказанных услугах, а также формирования отчётности для страховых организаций.

8.16. При выгрузке из МИС в 1С передаются:

– ФИО пациента, дата рождения, номер договора;

– перечень оказанных медицинских услуг с кодами и наименованиями по номенклатуре;

– стоимость оказанных услуг, сведения о применяемых скидках;

– сведения о форме оплаты;

– данные о датах оказания услуг и ответственных врачах (в части, необходимой для учёта).

8.17. При выгрузке в 1С передаётся исключительно информация, необходимая для учёта финансовых операций. Клинические данные (диагнозы, результаты анализов, медицинские заключения) в 1С не передаются и не хранятся, если это не обусловлено требованиями законодательства.

8.18. Доступ к выгружаемым данным в системе 1С разграничен в соответствии с должностными обязанностями сотрудников (ролевая модель доступа).

8.19. Регламент выгрузки данных утверждается отдельным Положением/Инструкцией

8.20. Обработка персональных данных в рамках интеграции МИС и 1С осуществляется на основании договора об оказании медицинских услуг с пациентом, требований Федерального закона от 06.12.2011 № 402-ФЗ «О бухгалтерском учёте», Налогового кодекса Российской Федерации в части требований к первичной документации.

8.6. В организации установлены следующие ограничения на распространение персональных данных:

– запрет трансграничной передачи;

– запрет передачи в рекламных целях — персональные данные пациентов не передаются третьим лицам для рекламных, маркетинговых или иных коммерческих целей без письменного согласия пациента.

– запрет передачи излишнего объёма данных — передача сведений, выходящих за рамки заявленной цели, не допускается.

9. Актуализация персональных данных

9.1. Актуализация персональных данных представляет собой комплекс мер, направленных на поддержание достоверности, точности и актуальности сведений о субъектах персональных данных, обрабатываемых Организацией.

Организация обязана обеспечивать соответствие обрабатываемых персональных данных их фактическому состоянию в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

9.2. Актуализация персональных данных осуществляется:

– по инициативе самого субъекта персональных данных;

– по инициативе Организации при выявлении недостоверных или устаревших сведений;

– на основании документов, поступивших от уполномоченных органов или организаций.

9.3. По заявлению субъекта персональных данных актуализация производится в связи с:

– изменение фамилии, имени, отчества (в связи с вступлением в брак, расторжением брака, иными обстоятельствами);

– изменение документа, удостоверяющего личность (паспортных данных);

– изменение адреса регистрации и/или фактического места проживания;

– изменение контактных данных (номера телефона, адреса электронной почты);

– изменение реквизитов страхового полиса ОМС или ДМС;

– изменение иных сведений, необходимых для оказания медицинской помощи.

9.4. По инициативе Организации актуализация производится в связи с:

– выявление ошибок, допущенных при первичном внесении данных в МИС;

– получение сведений об изменении данных из документов, предъявленных пациентом при обращении;

– уточнение данных при возникновении расхождений между сведениями в различных информационных системах (МИС, 1С, ЕГИСЗ);

– плановая проверка актуальности персональных данных в соответствии с утверждённым регламентом.

9.5. На основании документов государственных органов:

– уведомления органов ЗАГС об изменении персональных данных;

– сведений из Федеральной миграционной службы;

– иных официальных документов, подтверждающих изменение персональных сведений.

9.6. Субъект персональных данных вправе обратиться к Оператору с заявлением об уточнении или исправлении своих персональных данных.

Заявление подаётся:

– лично в регистратуре Организации;

– посредством направления заявления в письменной форме почтой России с уведомлением о вручении;

– посредством направления заявления в письменной форме, подписанного электронной цифровой подписью на электронную почту Организации.

При личном обращении пациент предъявляет документ, удостоверяющий личность, и/или иные документы, подтверждающие изменение сведений (свидетельство о браке, новый паспорт и пр.).

9.7. Организация обязана внести изменения в персональных данных в следующие сроки:

– при личном обращении пациента — в день обращения, незамедлительно при наличии подтверждающих документов;

– на основании письменного заявления — в течение 7 рабочих дней с момента его получения;

– при выявлении ошибки сотрудником Оператора — не позднее 3 рабочих дней с момента обнаружения.

9.8. После внесения изменений в МИС актуализированные персональных данных в установленном порядке передаются во все связанные информационные системы:

– в личный кабинет пациента — автоматически при синхронизации данных;

– в 1С — при очередной плановой выгрузке или внеплановой по запросу бухгалтерии;

– в ЕГИСЗ — в соответствии с требованиями Приказа Минздрава России от 07.09.2020 № 947н в установленные сроки.

9.9. Сотрудники ООО «МЦ НАИРИ МЕД» обязаны незамедлительно уведомлять специалиста по кадрам об изменении своих персональных данных и представить подтверждающие документы.

Специалист по кадровому учёту вносит изменения в личное дело сотрудника, кадровую систему и иные информационные ресурсы Оператора в течение 3 рабочих дней с момента представления документов.

Сведения о лицензиях, сертификатах и иных документах, подтверждающих квалификацию медицинских работников, актуализируются при прохождении очередного обучения, переаттестации либо при продлении/получении новых документов.

9.10. В целях обеспечения достоверности обрабатываемых персональных данных ООО «МЦ НАИРИ МЕД» проводит плановые проверки актуальности данных пациентов:

– при каждом обращении пациента за медицинской помощью сотрудник регистратуры обязан уточнить и при необходимости актуализировать контактные данные и сведения о документах пациента;

– не реже одного раза в год — сверка данных МИС с иными информационными системами (1С, кадровая система) в целях выявления расхождений.

По результатам плановой проверки составляется акт, фиксирующий выявленные расхождения и принятые меры по их устранению.

9.11. Все факты актуализации персональных данных фиксируются в:

– журнале учёта изменений персональных данных, который ведётся ответственным за обработку персональных данных;

– МИС — посредством автоматической фиксации истории изменений (логирование) с указанием даты, времени и учётной записи сотрудника, внёсшего изменения;

– личном деле пациента (бумажная амбулаторная карта) — путём внесения исправлений с подписью сотрудника и датой.

Журнал учёта хранится в течение 5 лет и предоставляется по запросу уполномоченных органов.

9.12. Ответственность за достоверность первичного внесения персональных данных несёт сотрудник, осуществивший их ввод в МИС.

Ответственность за организацию системы актуализации персональных данных в ООО «МЦ НАИРИ МЕД» несёт лицо, назначенное ответственным за организацию обработки персональных данных, в соответствии с приказом руководителя.

Субъект персональных данных несёт ответственность за своевременное уведомление Оператора об изменении своих сведений. Оператор не несёт ответственности за последствия, возникшие вследствие несвоевременного предоставления субъектом актуальных данных.

10. Уничтожение и удаление персональных данных.

10.1. Уничтожение персональных данных (далее — персональных данных) является одним из обязательных элементов жизненного цикла обработки персональных данных и осуществляется Организацией в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных», а также иных нормативных правовых актов.

10.2. Оператор обеспечивает уничтожение персональных данных:

– по истечении срока хранения, установленного законодательством или договором;

– при отзыве субъектом персональных данных согласия на обработку (если отсутствуют иные правовые основания);

– при достижении цели обработки персональных данных;

– по требованию уполномоченного органа (Роскомнадзора).

10.3. Персональные данные подлежат уничтожению до истечения установленного срока хранения в следующих случаях:

– отзыв согласия субъектом персональных данных. При поступлении от субъекта персональных данных заявления об отзыве согласия на обработку персональных данных, если отсутствуют иные законные основания для продолжения обработки (исполнение договора, требование законодательства, защита жизни и здоровья и пр.).

– требование субъекта персональных данных о прекращении обработки. При наличии доказательств незаконности обработки персональных данных либо при утрате Оператором необходимости в их обработке.

– предписания Роскомнадзора. При получении обязательного для исполнения предписания уполномоченного органа по защите прав субъектов персональных данных.

– достижение цели обработки. При достижении цели, для которой персональных данных были получены, если иное не предусмотрено договором или законодательством.

– истечение срока действия согласия. Если согласие на обработку было выдано на определённый срок и этот срок истёк.

10.4. Процедура уничтожения персональных данных инициируется на основании приказа Ответственного за обработку персональных данных.

10.5. Для проведения уничтожения персональных данных приказом руководителя Медицинского центра создаётся комиссия в составе не менее трёх человек.

10.6. Уничтожение персональных данных, обрабатываемых в МИС, 1С и иных информационных системах, осуществляется следующими способами:

– удаление записей из баз данных с последующей очисткой резервных копий;

– перезапись носителей информации с использованием сертифицированных программных средств (не менее трёх циклов перезаписи);

– физическое уничтожение носителей (жёстких дисков, иных носителей) в случае невозможности гарантированного программного уничтожения.

При уничтожении данных в информационных системах специалист по информационной безопасности обязан убедиться в удалении персональных данных из:

– основных баз данных информационных систем;

– резервных копий и архивов;

– журналов и логов (в части, содержащей персональных данных, не являющиеся необходимыми для аудита);

– временных файлов и кэша.

10.7. Документы, содержащие персональных данных (медицинские карты, договоры, заявления и пр.), уничтожаются путём:

– измельчения на шредере с уровнем защиты не ниже DIN 66399 P-4 (перекрёстная резка);

– передачи специализированной организации, имеющей соответствующую лицензию, для уничтожения с составлением акта приёма-передачи.

Категорически запрещается выбрасывать документы, содержащие персональных данных, без предварительного уничтожения.

10.8. Документы, содержащие персональные данные, подлежат уничтожению по истечение срока их хранения, за исключением случаев, когда уничтожение противоречит законодательству Российской Федерации.

Срок уничтожения персональных данных — не более 30 календарных дней дней с момента возникновения основания для их уничтожения.

10.9. По результатам уничтожения персональных данных комиссия составляет Акт об уничтожении персональных данных, который содержит:

– дату составления акта;

– перечень уничтоженных персональных данных (с указанием категорий субъектов, состава данных, периода обработки);

– сведения о носителях, на которых осуществлялось хранение (наименование информационной системы, тип носителя);

– применённый способ уничтожения;

– основание для уничтожения;

– подписи всех членов комиссии.

Акт об уничтожении персональных данных хранится у ответственного за организацию обработки персональных данных в течение 3 лет и предоставляется по запросу Роскомнадзора или субъекта персональных данных.

В течение 10 рабочих дней с момента уничтожения персональных данных Оператор уведомляет субъекта персональных данных (в случае, если уничтожение осуществлялось по его заявлению) о выполнении соответствующего требования.

10.10. При расторжении договора с подрядной организацией, которой были переданы персональных данных для обработки по поручению Организации, Организация обязана потребовать от подрядчика уничтожения переданных персональных данных в течение 30 рабочих дней с момента расторжения договора с предоставлением акта об уничтожении.

10.11. Данные, переданные в ЕГИСЗ, удаляются в порядке, установленном оператором ЕГИСЗ — Министерством здравоохранения Российской Федерации. Организация направляет соответствующий запрос в установленном порядке при наличии законных оснований.

10.12. Сведения, содержащиеся в данных бухгалтерского учёта в системе 1С, уничтожаются по истечении установленных сроков хранения первичных учётных документов с соблюдением требований законодательства о бухгалтерском учёте.

10.13. Ответственность за организацию и контроль соблюдения порядка уничтожения персональных данных возлагается на лицо, назначенное ответственным за организацию обработки персональных данных. Сотрудники ООО «МЦ НАИРИ МЕД», допустившие нарушения установленного порядка уничтожения персональных данных, несут дисциплинарную, административную и иную ответственность в соответствии с законодательством Российской Федерации.

11. Порядок взаимодействия с субъектами персональных данных.

11.1. Настоящий раздел устанавливает порядок взаимодействия ООО «МЦ НАИРИ МЕД» с субъектами персональных данных при поступлении обращений, запросов и заявлений, связанных с обработкой персональных данных, а также порядок регистрации таких обращений и сроки направления ответов.

ООО «МЦ НАИРИ МЕД» обеспечивает реализацию прав субъектов персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных нормативных правовых актов Российской Федерации.

Субъект персональных данных вправе обратиться в Организацию с запросами и заявлениями по следующим вопросам:

– получение сведений об обработке своих персональных данных;

– уточнение, исправление или дополнение персональных данных;

– отзыв согласия на обработку персональных данных;

– требование о прекращении обработки персональных данных;

– требование об уничтожении персональных данных;

– иные вопросы, связанные с обработкой персональных данных;

– предоставление копий документов, содержащих персональные данные субъекта.

11.2. Субъект персональных данных вправе направить обращение в ООО «МЦ НАИРИ МЕД» следующими способами:

– лично — путём обращения в регистратуру или к ответственному за организацию обработки персональных данных по адресу нахождения Организации. При личном обращении субъект персональных данных предъявляет документ, удостоверяющий личность (паспорт гражданина Российской Федерации либо иной документ, предусмотренный законодательством).

– почтовым отправлением — путём направления письменного заявления по почтовому адресу ООО «МЦ НАИРИ МЕД» заказным письмом с уведомлением о вручении. К заявлению прилагается нотариально заверенная копия документа, удостоверяющего личность заявителя.

– по электронной почте — путём направления заявления на официальный адрес электронной почты Организации.

При направлении обращения по электронной почте в обязательном порядке прилагаются:

– скан-копия или фотокопия паспорта гражданина Российской Федерации (либо иного документа, удостоверяющего личность), позволяющая однозначно идентифицировать заявителя;

– электронная подпись заявителя, проставленная на документе (заявлении). Принимается усиленная квалифицированная электронная подпись (УКЭП), полученная в удостоверяющем центре, аккредитованном в установленном порядке.

Обращения, поступившие по электронной почте без приложения копии документа, удостоверяющего личность, и/или без электронной подписи, Организацией не рассматриваются. Заявителю направляется уведомление о необходимости представить недостающие документы.

11.3. Обращение субъекта персональных данных должно содержать:

– фамилию, имя, отчество заявителя;

– номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем органе;

– сведения, подтверждающие отношение заявителя к ООО «МЦ НАИРИ МЕД» (пациент, бывший пациент, сотрудник и пр.);

– суть обращения (конкретное требование или вопрос);

– контактные данные для направления ответа (почтовый адрес и/или адрес электронной почты, номер телефона);

– подпись заявителя и дату составления обращения.

Если обращение подаётся законным представителем субъекта персональных данных, дополнительно прилагаются документы, подтверждающие полномочия представителя (нотариально удостоверенная доверенность, свидетельство о рождении — для родителей несовершеннолетних, и пр.).

11.4. Все поступившие обращения субъектов персональных данных подлежат обязательной регистрации в Журнале входящей корреспонденции (далее — Журнал) в день поступления обращения, а при поступлении в нерабочее время — в первый рабочий день, следующий за днём поступления.

Регистрацию обращений осуществляет администратор или регистратор ООО «МЦ НАИРИ МЕД», либо иной уполномоченный сотрудник.

Журнал ведётся в электронной форме и содержит следующие сведения:

– порядковый номер и дата регистрации обращения;

– фамилия, имя, отчество заявителя;

– способ поступления обращения (лично, почта, электронная почта, личный кабинет);
- суть обращения (краткое описание);

– отметка о комплектности документов (наличие копии паспорта, электронной подписи — для обращений по электронной почте);

– дата направления ответа;

– содержание принятого решения (краткое описание);

– подпись ответственного лица.

Заявителю при личном обращении выдаётся уведомление (отрывной талон, расписка) с указанием даты регистрации и входящего номера обращения. При поступлении обращения по почте или электронной почте уведомление о регистрации направляется заявителю в течение 3 рабочих дней с момента регистрации.

11.5. Сроки рассмотрения обращений составляет 10 календарных дней с даты регистрации обращения в соответствии с ч. 1 ст. 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

В случае если для рассмотрения обращения требуется запрос дополнительных сведений или проведение внутренней проверки, срок рассмотрения может быть продлён, но не более чем на 15 рабочих дней. О продлении срока заявитель уведомляется в письменной форме с указанием причин продления до истечения первоначального срока.

11.6. Ответ на обращение субъекта персональных данных направляется тем же способом, которым было подано обращение, либо способом, указанным заявителем в обращении.

Ответ должен содержать:

– ссылку на входящий номер и дату регистрации обращения;

– сведения о принятом решении с обоснованием;

– при полном или частичном отказе в удовлетворении требования — мотивированное обоснование отказа со ссылками на нормы законодательства;

– информацию о праве заявителя обратиться в надзорные органы или в суд для защиты своих прав.

Ответ подписывается руководителем ООО «МЦ НАИРИ МЕД» либо лицом, назначенным приказом Генерального директора, и заверяется печатью Организации (при направлении в бумажной форме) или усиленной квалифицированной электронной подписью (при направлении в электронной форме).

11.7. Организация вправе отказать в рассмотрении обращения по существу в следующих случаях:

– обращение не содержит сведений, позволяющих идентифицировать заявителя как субъекта персональных данных;

– к обращению, поступившему по электронной почте, не приложена копия паспорта и/или отсутствует электронная подпись заявителя;

– обращение подписано лицом, полномочия которого не подтверждены надлежащим образом;

– обращение содержит нецензурные выражения, оскорбления или угрозы в адрес сотрудников Организации.

Об отказе в рассмотрении обращения заявитель уведомляется в течение 3 рабочих дней с указанием причин отказа и разъяснением порядка повторного обращения.

11.8. Журнал, а также все поступившие обращения и копии ответов на них хранятся у лица, ответственного за организацию обработки персональных данных, в течение 3 лет с момента регистрации соответствующего обращения и предоставляются по запросу Роскомнадзора или суда.

12. Инциденты в области персональных данных и порядок реагирования на них

12.1. Настоящий раздел устанавливает порядок выявления, регистрации и реагирования на инциденты, связанные с нарушением безопасности персональных данных, обрабатываемых ООО «МЦ НАИРИ МЕД» (далее — Организация), а также порядок уведомления уполномоченных органов и субъектов персональных данных о произошедших инцидентах.

Организация руководствуется 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», а также Приказа Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия оператора с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций».

12.2. Инцидентом в области персональных данных признаётся любое событие, которое привело или могло привести к несанкционированному или случайному доступу к персональным данным, их уничтожению, изменению, блокированию, копированию, предоставлению, распространению, а также к иным неправомерным действиям в отношении персональных данных.

К инцидентам относятся, в том числе:

– несанкционированный доступ к информационным системам персональных данных (МИС, 1С, базам данных) со стороны внешних нарушителей (хакерские атаки, вредоносное программное обеспечение);

– несанкционированный доступ со стороны сотрудников Организации, превышение ими должностных полномочий;

– утрата, кража или утечка носителей персональных данных (ноутбуков, флеш-накопителей, распечатанных документов);

– случайное или умышленное уничтожение, изменение или блокирование персональных данных;

– передача персональных данных ненадлежащему получателю (ошибочная отправка по электронной почте, факсу, выдача медицинских документов постороннему лицу);

– сбои в работе информационных систем, повлёкшие утрату или компрометацию персональных данных;

– распространение персональных данных в сети Интернет или иных общедоступных источниках без законных оснований;

– нарушение работы средств защиты информации.

12.3. В ООО «МЦ НАИРИ МЕД» назначаются следующие ответственные лица:

– Ответственный за организацию обработки персональных данных — координирует деятельность по реагированию на инцидент, организует уведомление Роскомнадзора и субъектов персональных данных, ведёт документацию;

– Специалист по информационной безопасности (или уполномоченный сотрудник IT-службы) — осуществляет технический анализ инцидента, локализацию угрозы и восстановление систем;

– Руководитель Организации — принимает решения об уведомлении уполномоченных органов, субъектов персональных данных и иных заинтересованных сторон, санкционирует применение мер реагирования.

12.4. Любой сотрудник ООО «МЦ НАИРИ МЕД», обнаруживший признаки инцидента в области персональных данных или подозрительную активность, которая может к нему привести, обязан:

– немедленно прекратить действия, которые могут способствовать развитию инцидента (отключить устройство от сети, прекратить работу с информационной системой);

– незамедлительно — не позднее чем в течение 1 часа с момента обнаружения — сообщить об инциденте ответственному за организацию обработки персональных данных или его руководителю;

– зафиксировать обстоятельства обнаружения инцидента: время, место, характер нарушения, задействованные информационные ресурсы.

12.5. Сотруднику запрещается:

– самостоятельно предпринимать действия по ликвидации последствий инцидента без согласования с ответственным лицом;

– разглашать сведения об инциденте третьим лицам, не уполномоченным на получение такой информации;

– удалять или изменять данные, которые могут иметь доказательственное значение.

12.6. Реагирование на инцидент осуществляется поэтапно:

Этап 1. Первичная оценка (в течение 3 часов с момента обнаружения)

Ответственный за организацию обработки персональных данных совместно со специалистом по информационной безопасности проводят первичную оценку инцидента:

– устанавливают факт и природу инцидента;

– определяют перечень скомпрометированных персональных данных и круг затронутых субъектов персональных данных;

– оценивают возможный ущерб для субъектов персональных данных;

– принимают меры по локализации инцидента — блокированию несанкционированного доступа, изоляции поражённых систем, приостановке затронутых процессов обработки персональных данных.

Этап 2. Уведомление Роскомнадзора (не позднее 24 часов с момента обнаружения)

В соответствии с частью 3.1 статьи 21 Федерального закона № 152-ФЗ Организация направляет в Роскомнадзор уведомление об инциденте через портал «Госуслуги» или иной определённый уполномоченным органом способ. Уведомление содержит:

– дату и время обнаружения инцидента;

– описание обстоятельств инцидента;

– предполагаемые причины возникновения инцидента;

– сведения о категориях и приблизительном объёме скомпрометированных персональных данных;

– сведения о категориях затронутых субъектов персональных данных;

– меры, принятые или планируемые для устранения последствий инцидента;

– контактные данные ответственного лица.

Этап 3. Углублённое расследование (в течение 72 часов с момента обнаружения)

Специалист по информационной безопасности проводит детальный технический анализ инцидента:

– устанавливает точные причины и хронологию события;

– определяет полный перечень скомпрометированных персональных данных;

– оценивает наличие иных уязвимостей в инфраструктуре Организации.

По результатам расследования в Роскомнадзор направляется уточнённое уведомление не позднее 72 часов с момента первоначального обнаружения инцидента с актуализированными сведениями о его масштабах и последствиях.

Этап 4. Уведомление субъектов персональных данных

В случае если инцидент повлёк или мог повлечь нарушение прав субъектов персональных данных, Организация уведомляет затронутых субъектов в разумный срок способом, позволяющим подтвердить факт уведомления (электронная почта с уведомлением о доставке, SMS-сообщение, уведомление в личном кабинете, письмо с уведомлением о вручении). Уведомление содержит:

– описание произошедшего инцидента в форме, доступной для понимания;

– перечень персональных данных, которые были затронуты;

– рекомендации субъекту персональных данных по минимизации возможного ущерба (например, смена паролей, блокировка банковских карт при необходимости);

– контактные данные ответственного лица для обратной связи.

Этап 5. Устранение последствий и восстановление систем

Специалист по информационной безопасности совместно с IT-службой осуществляет:

– восстановление работоспособности информационных систем из резервных копий;

– устранение выявленных уязвимостей;

– проверку целостности данных после восстановления;

– усиление мер защиты с целью недопущения повторного инцидента.

12.7. Все инциденты в области персональных данных, независимо от их масштаба и последствий, подлежат обязательной регистрации в Журнале учёта инцидентов в области персональных данных (далее — Журнал инцидентов).

Журнал инцидентов содержит:

– порядковый номер и дату регистрации инцидента;

– дату и время обнаружения инцидента;

– описание инцидента и его предполагаемые причины;

– перечень скомпрометированных персональных данных и затронутых субъектов;

– принятые меры реагирования с указанием дат и ответственных лиц;

– сведения об уведомлении Роскомнадзора (дата и номер уведомления);

– сведения об уведомлении субъектов персональных данных;

– результаты расследования и итоговые выводы;

– меры, принятые для предотвращения повторных инцидентов.

Журнал инцидентов хранится у ответственного за организацию обработки персональных данных в течение 3 лет и предоставляется по запросу Роскомнадзора.

12.8. По результатам каждого зарегистрированного инцидента Организация проводит анализ причин его возникновения и разрабатывает план корректирующих мер, который может включать:

– внесение изменений в технические средства защиты информации;

– пересмотр прав доступа сотрудников к информационным системам;

– проведение внеплановых инструктажей и обучения сотрудников;

– обновление внутренних регламентов и инструкций в области обработки персональных данных;

– усиление контроля за действиями сотрудников в информационных системах.

12.9. Сотрудники ООО «МЦ НАИРИ МЕД», виновные в возникновении инцидента вследствие умышленных или халатных действий, а также не сообщившие об обнаруженном инциденте в установленные сроки, привлекаются к дисциплинарной, административной, гражданско-правовой или уголовной ответственности в соответствии с законодательством Российской Федерации.

13. Права субъектов персональных данных.

13.1. Настоящий раздел определяет перечень прав субъектов персональных данных при их обработке в ООО «МЦ НАИРИ МЕД», а также порядок реализации указанных прав.

13.2. Субъект персональных данных имеет право:

13.2.1. Получать информацию об обработке его персональных данных, включая:

– подтверждение факта обработки;

– цели обработки;

– способы обработки;

– сведения о лицах, имеющих доступ к данным;

– сроки обработки и хранения данных.

13.2.2. Требовать от Оператора:

– уточнения своих персональных данных;

– их блокирования или уничтожения — если данные неполные, устаревшие, неточные, незаконно получены или не являются необходимыми для заявленной цели обработки.

13.2.3. Отзывать согласие на обработку персональных данных (если обработка основана на согласии).

13.2.4. Обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

13.2.5. Требовать прекращения передачи (распространения, предоставления, доступа) своих персональных данных, если основание для такой передачи отсутствует.

13.2.6. В отношении медицинских данных:

– получать разъяснения о целях, объёме и способах обработки медицинских данных;

– требовать ограничения обработки медицинских данных, если это не требуется для оказания медицинской помощи или иных законных целей;

– запрашивать информацию о лицах (в том числе медицинских работниках), имеющих доступ к медицинским данным;

– требовать конфиденциального обращения с медицинскими данными, включая соблюдение врачебной тайны.

13.3. Субъект персональных данных обязан:

13.3.1. Предоставлять Оператору достоверные и актуальные персональные данные в случаях, когда это требуется для достижения целей обработки.

13.3.2. Своевременно информировать Оператора об изменении своих персональных данных, если это влияет на цели и условия их обработки.

14. Ответственность за нарушения в области обработки персональных данных.

14.1. Настоящий раздел устанавливает виды и меры ответственности, применяемые к ООО «МЦ НАИРИ МЕД» как юридическому лицу, а также к должностным лицам и сотрудникам Организации за нарушения требований законодательства Российской Федерации в области обработки и защиты персональных данных.

Ответственность за нарушения в области обработки персональных данных наступает в соответствии с:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Кодексом Российской Федерации об административных правонарушениях (статья 13.11 и смежные);

– Уголовным кодексом Российской Федерации (статьи 137, 138, 272, 274.1 и иные);

– Гражданским кодексом Российской Федерации (в части возмещения убытков и компенсации морального вреда);

– Трудовым кодексом Российской Федерации (в части дисциплинарной ответственности).

14.2. Административная ответственность наступает за нарушения, предусмотренные статьёй 13.11 Кодекса Российской Федерации об административных правонарушениях. Основные составы правонарушений и размеры санкций представлены в таблице ниже.

Помимо штрафа уполномоченный орган (Роскомнадзор) вправе выдать предписание об устранении выявленных нарушений, а в установленных законом случаях — обратиться в суд с требованием об ограничении доступа к информационным ресурсам Организации.

Состав правонарушения	Размер штрафа для юридических лиц
Обработка персональных данных в случаях, не предусмотренных законодательством, либо обработка, несовместимая с целями сбора	до 100 000 рублей (повторно — до 500 000 рублей)
Обработка персональных данных без письменного согласия субъекта	до 150 000 рублей (повторно — до 500 000 рублей)
Нарушение требований к локализации персональных данных граждан Российской Федерации на территории России	до 6 000 000 рублей (повторно — до 18 000 000 рублей)
Невыполнение обязанности по уточнению, блокированию или уничтожению недостоверных или незаконно полученных персональных данных	до 100 000 рублей
Неисполнение обязанности по уведомлению Роскомнадзора об обработке персональных данных	до 100 000 рублей
Невыполнение требований о защите персональных данных, повлёкшее несанкционированный доступ к ним	до 500 000 рублей (повторно — до 1 000 000 рублей)
Несоблюдение требований об уведомлении Роскомнадзора об инциденте в установленные сроки	до 3 000 000 рублей

14.3. К должностным лицам и сотрудникам Организации, виновным в умышленных нарушениях в области обработки персональных данных, может быть применена уголовная ответственность в соответствии с нормами Уголовного кодекса Российской Федерации.

14.3.1. Статья 137 УК РФ «Нарушение неприкосновенности частной жизни»:

– незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия — наказывается штрафом до 200 000 рублей, либо обязательными работами, либо лишением свободы на срок до 2 лет. При использовании служебного положения ответственность ужесточается.

14.3.2. Статья 272 УК РФ «Неправомерный доступ к компьютерной информации»:

– неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло её уничтожение, блокирование, модификацию либо копирование, — наказывается штрафом, либо исправительными работами, либо лишением свободы на срок до 2 лет (до 5 лет при наличии квалифицирующих признаков).

14.3.3. Статья 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»:

– применяется в случаях неправомерного разглашения содержания переписки или переговоров субъектов персональных данных.

14.4. Организация несёт гражданско-правовую ответственность перед субъектами персональных данных за вред, причинённый вследствие неправомерной обработки их персональных данных.

Субъект персональных данных вправе требовать в судебном порядке:

14.4.1. Возмещения убытков — реального ущерба и упущенной выгоды, понесённых вследствие нарушения его прав при обработке персональных данных (статья 15 Гражданского кодекса Российской Федерации).

14.4.2. Компенсации морального вреда — в размере, определяемом судом, вне зависимости от возмещения имущественного вреда и понесённых субъектом убытков (часть 2 статьи 24 Федерального закона № 152-ФЗ).

Организация освобождается от гражданско-правовой ответственности, если докажет, что вред возник вследствие непреодолимой силы или умысла самого субъекта персональных данных.

14.5. Сотрудники ООО «МЦ НАИРИ МЕД», допустившие нарушения требований законодательства Российской Федерации о персональных данных, а также внутренних нормативных документов Организации в области обработки персональных данных, привлекаются к дисциплинарной ответственности в порядке, установленном Трудовым кодексом Российской Федерации.

К нарушениям, за которые предусмотрена дисциплинарная ответственность, относятся:

– несоблюдение требований конфиденциальности персональных данных, ставших известными сотруднику в связи с исполнением должностных обязанностей;

– разглашение персональных данных коллег, пациентов или иных субъектов персональных данных третьим лицам без законных оснований;

– несанкционированное копирование, передача или использование персональных данных в целях, не связанных с исполнением должностных обязанностей;

– непринятие мер при обнаружении инцидента в области персональных данных или несвоевременное уведомление ответственных лиц;

– нарушение установленного порядка работы с информационными системами, содержащими персональные данные.

За совершение указанных нарушений к сотруднику могут быть применены следующие дисциплинарные взыскания:

– замечание;

– выговор;

– увольнение по основаниям, предусмотренным Трудовым кодексом Российской Федерации (в частности, пункт 6 части 1 статьи 81 — разглашение охраняемой законом тайны, ставшей известной работнику в связи с исполнением трудовых обязанностей).

Привлечение сотрудника к административной или уголовной ответственности не освобождает его от дисциплинарной ответственности.

14.6. Лицо, назначенное приказом руководителя ООО «МЦ НАИРИ МЕД» ответственным за организацию обработки персональных данных, несёт персональную ответственность за:

– надлежащую организацию системы обработки и защиты персональных данных в Организации;

– своевременное уведомление Роскомнадзора об инцидентах в установленные сроки;

– соответствие принятых мер защиты требованиям действующего законодательства;

– ведение документации в области персональных данных в актуальном состоянии;

– проведение обучения и инструктажа сотрудников по вопросам обработки персональных данных.

14.7. При выявлении нарушений требований в области обработки персональных данных Организация соблюдает следующий порядок:

– фиксация факта нарушения (служебная записка, акт, уведомление от контролирующего органа);

– проведение внутреннего расследования с установлением обстоятельств нарушения и виновных лиц;

– принятие мер по устранению нарушения и его последствий;

– применение к виновным лицам мер дисциплинарного воздействия;

– направление информации в правоохранительные органы при наличии признаков уголовно наказуемого деяния.

Привлечение сотрудника к ответственности за нарушение требований в области обработки персональных данных не освобождает Организацию от ответственности, установленной законодательством Российской Федерации.