УТВЕРЖДАЮ
Директор ООО "Центр современной стоматологии доктора Лоншакова"



Лоншаков С. П.
15 января 2025 г.

Порядок информационной безопасности информационной системы по обработке персональных данных в ООО "Центр современной стоматологии доктора Лоншакова"

1. Термины и определения

Безопасность информации ограниченного доступа - состояние защищенности информации ограниченного доступа, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах с информацией ограниченного доступа.

Доступ к информации - возможность получения информации и ее использования.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информация ограниченного доступа - любая информация, отнесенная к конфиденциальной информации, а именно: персональные данные, служебная тайна, врачебная тайна или иная информация, доступ к которой ограничен в соответствии с нормативно-правовыми актами Российской Федерации.

Информационная система с информацией ограниченного доступа - информационная система, представляющая собой совокупность информации ограниченного доступа, содержащихся в базе данных или в виде отдельных файлов с данными, а также информационных технологий и технических средств, позволяющих осуществлять обработку такой информации с использованием средств автоматизации или без использования таких средств.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно

нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Неправомерные действия с информацией ограниченного доступа - преднамеренное или случайное несанкционированное ознакомление с информацией ограниченного доступа, ее копирование, распространение, передача, уничтожение, изменение (модификация), блокирование, а также любое иное несанкционированное использование, которое может нанести ущерб Обществу или государству.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа.

Обработка информации ограниченного доступа - действия (операции) с информацией ограниченного доступа, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение.

Пароль - секретная (конфиденциальная) строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системы для получения доступа к данным и программам; является средством защиты данных от несанкционированного доступа.

Пользователь - работник, использующий ресурсы информационной системы для выполнения должностных обязанностей.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Распространение информации ограниченного доступа - действия, направленные на передачу такой информации определенному кругу лиц или на ознакомление с информацией ограниченного доступа неограниченного круга лиц, в том числе ее обнародование в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ней каким-либо иным способом.

Технические средства информационной системы - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации ограниченного доступа (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2. Общие положения

2.1. Настоящий Порядок информационной безопасности информационной системы по обработке персональных данных (далее - Порядок) составлен в соответствии с п. 2 ст. 18.1 Федерального закона РФ «О персональных данных» №152-ФЗ от 27.07.2006 г. и действует в отношении персональных данных (далее - ПДн), которые ООО "Центр современной стоматологии доктора Лоншакова" (далее - Учреждение), может получить от субъекта персональных данных или из общедоступных источников, в рамках выполнения основной деятельности Учреждения.

2.2. Порядок распространяется на ПДн полученные как до, так и после подписания настоящего Порядка.

2.3. Необходимость разработки настоящего Порядка обусловлена применением новейших информационных технологий и процессов при

обработке информации вообще, и информации ограниченного доступа в частности.

2.4. Законодательной основой настоящего Порядка являются Конституция Российской Федерации, Трудовой кодекс Российской Федерации, федеральные законы Российской Федерации, Указы и распоряжения Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, другие нормативные документы действующего законодательства Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

2.5. Областью применения являются работники Учреждения, а также лица, состоящие в договорных отношениях с Учреждением, подразумевающих исполнение требований настоящего Порядка и имеющие доступ к информационным ресурсам Учреждения.

3. Персональные данные обрабатываемые в ООО "Центр современной стоматологии доктора Лоншакова"

3.1. Учреждение обрабатывает следующие категории персональных данных:

а) персональные данные граждан, обратившихся за медицинской помощью в Учреждение (далее - Пациенты);

б) персональные данные работников Учреждения (далее - Работники);

3.2. К персональным данным Пациентов относятся:

— Фамилия, Имя, Отчество;
— Год, месяц и число рождения;
— Место рождения;
— Паспортные данные (номер, серия, дата и место выдачи);
— Адрес прописки и адрес проживания;
— Номер телефона (мобильный/домашний);
— Сведения о медицинском полисе ДМС;
— Информация о состоянии здоровья.

3.3. К персональным данным Сотрудников относятся:

— Фамилия, Имя, Отчество;
— Год, месяц и число рождения;
— Место рождения;
— Паспортные данные (номер, серия, дата и место выдачи);
— Адрес прописки и адрес проживания;
— Семейное положение;
— Номер телефона (мобильный/домашний);
— Состав семью (супруги, дети);
— Социальное положение;
— Информация о состоянии здоровья;
— Сведения об образование;
— Сведения о профессии;
— Сведения о доходах;
— ИНН / СНИЛС;
— Сведения о воинском учете.

4. Цель сбора и обработки персональных данных субъектов ПДн

4.1. Учреждение осуществляет обработку персональных данных Пациентов для предоставления медицинских консультативно - диагностических услуг (далее - медицинская помощь) и ведения учета пациентов в установленном порядке.

4.2. Учреждение осуществляет обработку персональных данных Работников для выполнения требований Трудового кодекса Российской Федерации, автоматизации и совершенствования деятельности кадровой службы Учреждения.

5. Условия обработки персональных данных и их передачи третьим лицам

5.1. Учреждение вправе передать ПДн третьим лицам в случаях, предусмотренных законодательством Российской Федерации.

5.2. При обработке ПДн пациентов и работников Учреждения, Учреждение руководствуется следующими нормативно-правовыми актами:

— Федеральным законом РФ от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

— Федеральным законом от 27.07.06г. № 152-ФЗ «О персональных данных»;

— Федеральным законом от 27.07.06г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

— Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации, необходимые для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защиты»;

— Внутренними утвержденными нормативными документами Учреждения.

6. Меры обеспечения информационной безопасности

Учреждение принимает необходимые, достаточные технические и

организационные меры для защиты ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ней со стороны третьих лиц.

6.1. Размещение информации на официальных информационных ресурсах

Официальные материалы, подлежащие размещению на официальных информационных ресурсах Учреждения. Дополнительно допускается размещение в прочих официальных информационных ресурсах.

Содержание официальных материалов должно удовлетворять требованиям нормативно-правовых актов Российской Федерации. Ответственность за соответствие содержания официальных материалов требованиям нормативно-правовых актов Российской Федерации возлагается на работника, уполномоченного и согласовавшего размещение таковых материалов.

Размещение официальных материалов на официальных интернет - порталах осуществляется Учреждением самостоятельно, за исключением случаев, предусмотренных прочими нормативными документами.

Содержание официальных материалов должно быть общедоступно и содержать свободно распространяемую информацию.

Размещение в официальных материалах информации (материалов) из сторонних источников (авторов) должно осуществляться с соблюдением требований нормативно-правовых актов Российской Федерации в сфере защиты авторских прав и интеллектуальной собственности.

В соответствии с нормативными правовыми актами Российской Федерации публикация в официальных материалах информации ограниченного доступа и составляющих государственную тайну запрещена.

Обладателем информации, публикуемой на официальных интернет - порталах, является Учреждение, предоставляющее данные материалы.

6.2. Использование программного обеспечения

Программное обеспечение, используемое для осуществления деятельности Учреждения, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением. Случаи хранения и/или использования программного обеспечения, не являющегося лицензионным, должны быть исключены.

В случае, если нормативно-правовыми актами Российской Федерации предъявляются особые требования к программному обеспечению (например, требование по сертификации такого программного обеспечения

уполномоченными организациям и т.п.) необходимо обеспечить выполнение таких требований.

На каждое автоматизированное рабочее место должен быть установлен комплект программного обеспечения, необходимый и достаточный для выполнения на нем поставленных задач.

6.3. Обеспечение физической безопасности

Все помещения Учреждения в которых ведется обработка ПДн субъектов должны отвечать требованиям нормативно-правовых актов Российской Федерации в части оборудования устройствами сигнализации (пожарной, охранной и т.п.).

Все помещения Учреждения должны быть оборудованы дверьми, закрываемыми на замок.

Во всех помещениях Учреждения, должна иметься возможность организации круглосуточной охраны.

Работники не должны оставлять свои рабочие кабинеты без наблюдения. В случае, если помещение остается без наблюдения, помещение должно быть закрыто на замок.

6.4. Парольная защита

Доступ к программному обеспечению, используемому пользователями и системными администраторами в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и/или разграничение полномочий без использования пароля запрещено.

Пароли доступа к различному прикладному программному обеспечению, используемому пользователями и администраторами в рамках должностных обязанностей должны отличаться от паролей доступа к автоматизированному рабочему месту или элементам сетевой инфраструктуры и не должны совпадать для различного программного обеспечения. Допускается совпадение паролей для программного обеспечения использующего для идентификации и аутентификации учетные записи в Active Directory.

В качестве паролей допускается использование только устойчивых паролей.

Работникам Учреждения, исполняющим обязанности системных администраторов и администраторов информационной безопасности запрещено отклоняться от настоящего Порядка в целях удобства пользования.

6.5. Обеспечение антивирусной защиты

Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех АРМ, серверах и портативных устройствах Учреждения (в программном исполнении).

6.6. Межсетевое экранирование

Для обеспечения информационной безопасности при присоединении к сетям общего пользования (далее - СОП), а так же к локальным сетям

сторонних организаций, такие присоединения должны быть защищены межсетевыми экранами (далее МЭ), не зависимо от используемых технологий подключения (например, подключение с использование беспроводных сетей, модемов и т.п.), отвечающих требованиям нормативноправовых актов Российской Федерации.

Допускается установка межсетевого экрана как с группировкой АРМ по типу обрабатываемой информации и отделение ИСПДн, так и установка персональных межсетевых экранов на каждое АРМ.

6.7. Использование сетей общего пользования

Учреждение не несет ответственности за информацию, содержащуюся в сетях общего пользования. В случае открытия пользователем ресурсов, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, пользователь обязан прекратить работу с данным ресурсом.

Для получения возможности доступа пользователя в сети общего пользования необходимо использование технологий идентификации и аутентификации, а также должны быть обеспечены механизмы защиты информационных ресурсов Учреждения от воздействия из сетей общего пользования.

Пользователям запрещено использование любых способов доступа в сети общего пользования (например, dial-up доступ, использование для соединения с СОП операторов сотовой связи и т.п.) отличных от установленных.

Передача информации ограниченного доступа по сетям общего пользования, допускается при условии соблюдения всех требований, определяемых нормативными правовыми актами Российской Федерации, к такой передаче.

Пользователям запрещается при работе в СОП передавать конфиденциальные данные, не прошедшие криптографическое преобразование и допускать просмотра их третьими лицами. Передача информации ограниченного доступа без соблюдения требований, предъявляемых к ее передаче по СОП, запрещена.

Пользователю запрещено любое тестирование и/или попытки обхода установленных механизмов защиты.

Доступ в сети общего пользования сотрудникам Учреждения предоставляется только после согласования с руководством и лицом ответственным за обработку персональных данных в Учреждении.

Получение доступа пользователя к ресурсам сети общего пользования, не означает, что пользователь имеет неограниченные возможности при работе

с данным ресурсом. Уполномоченными работниками Учреждения могут приниматься меры по предотвращению отдельных действий пользователя при работе с ресурсами сетей общего пользования, как-то ограничение по загрузке отдельных файлов, отображение объявлений рекламного, порнографического и иного характера и т.п.

Использование ресурсов Учреждения для участия в игровых, развлекательных и иных ресурсах (включая конкурсы, выставки, социальные сети и иные Интернет-сообщества) запрещено. Если иное не разрешено руководством Учреждения.

Пользователям запрещено размещать любую информацию о деятельности Учреждения в СОП, кроме информации, размещаемой в соответствии с требования нормативно-методических документов Российской Федерации или требующие выполнение функций и обязанностей Учреждения.

В целях выявления нецелевого использования ресурсов, Учреждение может собирать информацию о посещенных пользователем ресурсах сетей общего пользования, загруженных файлах, времени проведенном на отдельных ресурсах сетей общего пользования и иной связанной информации. Данная информация может быть использована для анализа использования пользователем сетей общего пользования в соответствии с предоставленными ему полномочиями, в рамках выполнения пользователем своих должностных обязанностей.

В любое время, без предварительного предупреждения, работник ответственный за информационную безопасность Учреждения в праве провести анализ передаваемых электронных сообщений, содержимого log-файлов, файлов, размещенных на автоматизированном рабочем месте пользователя, их настройку и конфигурацию, установленного на них программного обеспечения, а также любой другой информации находящейся на автоматизированном рабочем месте пользователя или передаваемой по локальным вычислительным сетям Учреждения или за ее пределы.

6.8. Использование электронной почты

Все системы электронной почты должны быть использованы пользователями только для выполнения должностных обязанностей, выполнения договорных обязательств и выполнения требований нормативных правовых актов Российской Федерации.

Запрещено использовать электронную почту для отправления писем следующего содержания:

- писем, содержание которых может считаться незаконным или оскорбительным, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные,

дискриминационные, угрожающие, или иные подобные сообщения;

- любых подрывных, оскорбительных, неэтичных, незаконных или иначе недопустимых материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возрасте, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений или о национальном происхождении, гиперссылок или других ссылок на неприличные или очевидно оскорбительные веб-сайты и подобные материалы, шутки, массовые рассылки, предупреждений о вирусах и розыгрышей, обращений о помощи или вредоносного кода;

- писем, написанных таким образом, который может быть интерпретирован как официальная позиция или высказывание Учреждения, если это не разрешено в соответствии с нормативно-методическими документами Учреждения.

- отправки сообщения с чужого почтового ящика или от чужого имени;

- отправки сообщений в личных целях, не связанных с задачами Учреждения;

- массовой рассылки писем, кроме случаев когда необходимо оповещение большого числа работников и пациентов Учреждения или в случаях когда это обусловлено выполнением функций и задач Учреждения;

- в любых других незаконных, неэтичных и неразрешенных целях.

- В исключительных случаях, пользователь может принять решение об использовании системы электронной почты, отличной от корпоративной. При этом должны выполняться остальные положения настоящего Порядка и требования нормативно-правовых актов Российской Федерации и организационно-распорядительные документы Учреждения.

- Пользователям запрещено отвечать на запросы любой персональной идентификационной информации, включая пароли, коды доступа, номера кредитных карт и т.п. В случае получения сообщений с такими запросами пользователь обязан сообщить о них работнику ответственному за информационную безопасность Учреждения.

Отправка электронной почты, содержащей информацию ограниченного доступа, должна осуществляться в соответствии с требованиями, предъявляемыми к такой информации.

Отправка персональных данных по средствам электронном почты без использования криптографических средств запрещена.

6.9. Использование средств криптографической защиты информации

Использование СКЗИ должно быть обусловлено требованиями нормативно-методических документов Российской Федерации и/или в соответствии с моделью нарушителя.

Деятельность с СКЗИ должна исключать нарушение законодательства Российской Федерации в области лицензирования. В случае, если предполагаемая деятельность с СКЗИ подразумевает необходимость получения лицензии, Учреждение обязано получить такую лицензию или привлекать для подобной деятельности сторонние организации, имеющие соответствующие лицензии.

При использовании СКЗИ для защиты информации ограниченного доступа данные криптографические средства должны соответствовать требованиям нормативно-правовых актов Российской Федерации, требованиям регулятора в области криптографии, в том числе к их классу и сертификации.

6.10. Использование переносных устройств

Под переносным устройством понимается любое устройство обработки информации в электронном виде, по особенностям своей конструкции, предназначенные для обработки информации без привязки к определенному месту (ноутбуки, планшеты, видеокамеры, смартфоны и т.п.).

Использование работниками личных переносных устройств для выполнения должностных обязанностей запрещено (за исключением случаев совершения телефонных звонков по личным сотовым телефонам).

Подключение личных переносных устройств к локальным вычислительным сетям Учреждения запрещено.

Служебные переносные устройства должны отвечать требованиям настоящего Порядка, включая требования по парольной защите, антивирусной защите, установленному программному обеспечению, использованию СКЗИ и т.п. Служебные переносные устройства, не отвечающие требованиям настоящего Порядка, запрещено использовать для выполнения должностных обязанностей работниками, в том числе подключать их к локальным вычислительным сетям и другим устройствам Учреждения.

Работник, использующий служебные переносные устройства, несет персональную ответственность за обеспечение их сохранности. Работникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными переносными устройствами.

Использование служебных переносных устройств в личных целях, а также для совершения противоправных действий запрещено.

6.11. Требования при выполнении должностных обязанностей

Ответственное выполнение требований по информационной безопасности является обязанностью всех работников Учреждения. Требования по информационной безопасности касаются всех работников Учреждения.

Для выполнения требований по информационной безопасности работники должны знать требования нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения, регламентирующие данные требования и письменно подтверждать свое согласие на их выполнение.

При поступление на работу сотрудника служебные обязанности которого связаны с обработкой конфиденциальных данных, он обязан пройти инструктаж у ответственного лица по защите информации.

При увольнении или прекращении договорных обязательств работники должны быть уведомлены и согласны с требованиями по неразглашению информации ограниченного доступа и сведений о системе защиты информации, в соответствии с требованиями нормативно-правовых актов Российской Федерации и организационно-распорядительной документации Учреждения.

В Учреждении должны производится периодические мероприятия направленные на постоянное повышение осведомленности работников в области информационной безопасности.

Работник, чьи должностные обязанности предполагают выполнение работ по созданию, настройке, сопровождению и совершенствованию системы по обеспечению информационной безопасности, должны проходить специализированное обучение по данным направлениям.

7. Изменение персональных данных

Субъекты ПДн имеют право требовать внесение изменений и дополнений своих ПДн, обрабатываемых в Учреждение, обратившись к лицу, ответственному за организацию обработки ПДн, при этом они должны иметь оригиналы подтверждающих документов, в соответствии с которыми вносятся изменения.

8. Внесение изменений в Порядок

Учреждение имеет право вносить изменения в настоящий Порядок в случае изменение в нормативно-правовых актах Российской Федерации и организационно - распорядительной документации Учреждения.

Новая редакция Порядка вступает в силу с момента ее подписания руководителем Учреждения, если иное не предусмотрено новой редакцией Порядка.

9. Ответственность

Ответственность за нарушение требований настоящего Порядка накладывается на работников Учреждения, подразумевающих исполнение требований Порядка, совершивших нарушения, в зависимости от категории

нарушения, возникшего в результате необеспечения или нарушения требований настоящего Порядка, и величины причиненного ущерба (нежелательных последствий).

Указанные категории лиц могут привлекаться к дисциплинарной ответственности.

10. Обратная связь

Функции по защите информации возложены на руководство Учреждения

Адрес электронной почты: doclonshakov@mail.ru

Почтовый адрес: 625023, ТЮМЕНСКАЯ ОБЛАСТЬ, Г. ТЮМЕНЬ, УЛ. 50 ЛЕТ ОКТЯБРЯ, Д. 57В, ПОМЕЩ. 4

Контактный телефон: 83452706670