Приложение №1
к приказу ГАУ РО «ОКДЦ»
№ 301 от «01» июля 2025 г.

ПОЛИТИКА
обработки персональных данных в ГАУ РО «ОКДЦ»

1. Общие положения

1.1 Настоящая Политика обработки персональных данных (далее – Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и определяет ключевые направления деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является ГАУ РО «ОКДЦ» (далее – Центр, Оператор).

1.2 Политика разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки ПДн субъектов персональных данных.

1.3 Политика раскрывает правовые основания, цели обработки персональных данных, категории обрабатываемых ПДн и источники их получения, основные принципы обработки, передачи и хранения персональных данных, меры по обеспечению безопасности ПДн при их обработке Оператором, а также права субъектов персональных данных.

1.4 Принятие настоящей политики преследует следующие цели:

обеспечение защиты прав и свобод субъектов ПДн при обработке их ПДн Оператором;

предотвращение нарушений законных прав и интересов субъектов персональных данных;

защита ПДн субъектов ПДн от несанкционированного доступа и разглашения;

недопущение нанесения возможного ущерба, вызванного неправомерными умышленными или неосторожными действиями юридических и (или) физических лиц путем безвозмездного присвоения информации или ее разглашения, нарушением установленных норм, регулирующих обработку и защиту персональных данных.

1.5 Основные понятия, используемые в настоящей Политике:

ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

обработка ПДн – 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;

распространение ПДн – действия, направленные на раскрытие ПДннеопределенному кругу лиц;

предоставление ПДн – действия, направленные на раскрытие ПДн

определенному лицу или определенному кругу лиц;

блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

2. Правовые основы обработки персональных данных

Политика Центра в области обработки ПДн определяется следующими основными нормативными правовыми актами Российской Федерации:

Конституцией Российской Федерации;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах персональных данных»;

Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных»;

Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации».

3. Цели обработки персональных данных

3.1 Обработка ПДн работников осуществляется с целью исполнения трудовых договоров, заключенных между Центром и субъектами ПДн в соответствии с требованиями законодательства Российской Федерации.

3.2 Обработка ПДн пациентов осуществляется с их предварительного согласия с целью оказания медицинских услуг.

3.3 Обработка и хранение ПДн осуществляются не дольше, чем этого требуют цели обработки персональных данных, указанные в пп. 3.1. и 3.2. настоящей Политики, если отсутствуют законные основания для их дальнейшей обработки или в соответствии со сроками, указанными в отдельных нормативных правовых актах Российской Федерации.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию при наступлении следующих условий:

при достижении цели обработки персональных данных, если иное не

предусмотрено договором – в течение 30 дней;

предоставление субъектом ПДн или его законным представителем подтверждения того, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки – в течение 7 дней;

невозможность обеспечения правомерности обработки ПДн – в течение 10 рабочих дней;

отзыв субъектом ПДнсогласия на обработку персональных данных, если сохранение ПДн более не требуется для целей обработки ПДн – в течение 30 дней;

ликвидация Центра.

3.4 В случае отсутствия возможности уничтожения ПДн в течение сроков, указанных в п. 3.3. настоящей Политики, Оператор осуществляет блокирование таких ПДн и обеспечивает уничтожение ПДн в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

4. Категории обрабатываемых персональных данных, источники их получения

4.1 В информационных системах ПДн Центра обрабатываются следующие категории персональных данных:

персональные данные работников Центра;

персональные данные пациентов;

специальная категория ПДн (врачебная тайна).

4.2 Для достижения целей обработки ПДн Оператор обрабатывает следующие персональные данные работников:

фамилия, имя, отчество;

пол;

возраст;

дата рождения;

место рождения;

гражданство;

паспортные данные;

адрес регистрации по месту жительства и адрес фактического проживания;

номер телефона (домашний, мобильный);

адрес электронной почты;

данные документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, аттестации, аккредитации, подтверждении специальных знаний, присвоении ученой степени, ученого звания, сведения о наградах и званиях (при наличии);

семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления льгот, предусмотренных трудовым и налоговым законодательством;

данные документов воинского учета (для военнообязанных и лиц, подлежащих призыва на военную службу);

наименование должности;

сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

данные страхового свидетельства государственного пенсионного

страхования (СНИЛС);

данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (ИНН);

фотография (для оформления личных карточек, личных дел, пропусков, размещения на сайте Центра, в информационных сообщениях в СМИ всех видов, на стендах и информационных досках внутри Центра);

информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности;

сведения о заработной плате (доходах), банковских счетах, картах;

сведения о деловых и иных личных качествах, носящих оценочный характер;

сведения о социальных льготах, пенсионным обеспечении и страховании;

данные документов об инвалидности (при наличии);

данные страхового медицинского полиса обязательного медицинского страхования;

медицинское заключение;

иные персональные данные в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, необходимые для достижения целей, предусмотренных пп. 3.1. и 3.2. настоящей Политики.

4.3 Персональные данные работников предоставляются самими работниками.

4.4 Для достижения целей обработки ПДн Оператор обрабатывает следующие персональные данные пациентов, а также сведения, содержащие врачебную тайну:

фамилия, имя, отчество;

пол;

дата рождения;

место рождения;

гражданство;

данные документа, удостоверяющего личность;

место жительства;

место регистрации;

адрес электронной почты;

данные страхового свидетельства государственного пенсионного страхования (СНИЛС);

данные полиса обязательного медицинского страхования застрахованного лица (при наличии);

анамнез;

диагноз;

вид оказанной медицинской помощи;

объем оказанной медицинской помощи;

результат обращения за медицинской помощью;

серия и номер выданного листа нетрудоспособности (при наличии);

сведения об оказанных медицинских услугах;

примененные стандарты медицинской помощи;

иные персональные данные в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, необходимые для достижения целей, предусмотренных пп. 3.1. и 3.2. настоящей Политики.

4.5 ПДн пациентов могут быть получены от них лично в заполненной анкете или в ходе личного опроса.

5. Основные принципы обработки, передачи и хранения персональных данных

5.1 Обработка ПДн осуществляется на законной и справедливой основе.

5.2 Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

5.3 Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

5.4 Допускается обработка только тех ПДн, которые отвечают целям их обработки.

5.5 Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

5.6 При обработке ПДн, Оператором должна быть обеспечена точность обрабатываемых ПДн, их достаточность и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры, либо обеспечивать их принятие, по удалению, уточнению неполных или неточных ПДн.

5.7 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен нормативными правовыми актами Российской Федерации, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами и другими нормативными правовыми актами Российской Федерации.

5.8 Оператор в установленном порядке вправе поручить обработку ПДн субъектов ПДн третьим лицам. При этом существенным условием договора является требование по обеспечению безопасности ПДн.

5.9 В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов ПДн (работников) Оператор в ходе своей деятельности, на основании письменного запроса, предоставляет ПДн следующим организациям:

Федеральной налоговой службе;

Социальному фонду России;

Негосударственным пенсионным фондам;

Территориальному Фонду обязательного медицинского страхования;

Федеральной миграционной службе;

Кредитным организациям (для реализации зарплатных проектов и выполнения договорных обязательств);

Лицензирующим и (или) контролирующим органам государственной власти и местного самоуправления;

Иным организациям, определенным действующим законодательством Российской Федерации.

5.10 В договоры с лицами, которым Оператор поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные Федеральным законом от 27 июля 2006 г. № 152 «О персональных данных» правила обработки ПДн.

6. Меры по обеспечению безопасности персональных данных при их обработке

6.1 Центр при обработке ПДн принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

6.2 Приказом главного врача назначается лицо, ответственное за организацию обработки ПДн Оператором.

6.3 Ответственное лицо осуществляет внутренний контроль и (или) аудит соответствия применяемых Оператором мер по защите ПДн требованиям нормативных правовых актов Российской Федерации.

6.4 Доступ работников к обрабатываемым ПДн организован в соответствии с их должностными обязанностями и регламентирован требованиями локальных документов Центра.

6.5 Работники Центра, непосредственно осуществляющие обработку ПДн, знакомятся с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами организации в отношении обработки ПДн под подпись.

6.6 При обработке ПДн в информационных системах применяются необходимые организационные и технические меры по обеспечению их безопасности.

6.7 Осуществляется оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн.

6.8 Организован и ведется учет машинных носителей ПДн.

6.9 Установлены правила доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечены регистрация и учет всех действий, совершаемых с ПДн в информационной системе персональных данных.

6.10 При обработке ПДн субъектов ПДн используются базы данных, находящиеся на территории Российской Федерации.

7. Права субъектов персональных данных

7.1 Субъект ПДн имеет право на получение сведений об обработке своих ПДн Оператором.

7.2 Субъект ПДн вправе требовать от Оператора уточнения, при необходимости, своих ПДн, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.3 Субъект ПДн имеет право на защиту своих прав и законных интересов.

7.4 Право субъекта ПДн на доступ к его персональным данным может быть

ограничено в соответствии с требованиями федеральных законов Российской Федерации.

7.5 Центр рассматривает любые обращения и жалобы со стороны субъектов ПДн, расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке. Все запросы и обращения субъектов ПДн регистрируются в «Журнале учета обращений субъектов персональных данных».

7.6 Субъект ПДн вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов ПДн.

8. Обязанности оператора

8.1 Предоставлять субъекту ПДн по его запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

8.2 Разъяснить субъекту ПДн юридические последствия отказа предоставить персональные данные, если предоставление ПДн является обязательным в соответствии с Федеральным законом.

8.3 Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.4 В соответствии с ч. 2 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152 «О персональных данных» опубликовать в сети Интернет на официальном сайте «http://rokdc.ru/» и обеспечить неограниченный доступ с использованием сети Интернет к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.

8.5 Осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к субъекту ПДн или обеспечить их блокирование, если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора.

8.6 Уточнять персональные данные субъектов ПДн, либо обеспечить их уточнение, если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора.

8.7 В случае выявления неправомерной обработки ПДн, осуществляемой Оператором или лицом, действующим на основании договора с Оператором, прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Оператора.

8.8 Прекратить обработку ПДн или обеспечить ее прекращение, если обработка ПДн осуществляется другим лицом, действующим по договору с Оператором. Уничтожить данные или обеспечить их уничтожение, если ПДн осуществляется другим лицом, по поручению Оператора, по достижению цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, в случае достижения цели обработки ПДн.

8.9 Прекратить обработку ПДн или обеспечить ее прекращение и уничтожить ПДн или обеспечить их уничтожение в случае отзыва субъектом ПДн

согласия на обработку ПДн.

8.10 Выполнять иные обязанности, предусмотренные законодательством Российской Федерации.

8.11 Работники Центра обязаны:

ознакомиться с Политикой и внутренними документами, регламентирующими процесс обработки ПДн, и выполнять требования этих документов;

обрабатывать ПДн только в рамках выполнения своих должностных обязанностей;

не разглашать ПДн, к которым был получен доступ в рамках исполнения своих трудовых обязанностей;

информировать работодателя о фактах разглашения (уничтожения, искажения) ПДн.

9. Заключительные положения

9.1 Политика является общедоступным документом и подлежит размещению в доступном для субъектов ПДн месте.

9.2 Политика подлежит изменению (дополнению) в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите ПДн, но не реже одного раза в три года.

9.3 Контроль исполнения требований настоящей Политики осуществляется должностным лицом Центра, ответственным за организацию обработки ПДн.

9.4 Ответственность за невыполнение требований, регулирующих обработку и защиту ПДн, должностными лицами Центра, имеющими доступ к ПДн, определяется в соответствии с законодательством Российской Федерации и внутренними локальными документами.

Приложения:

1. Типовые запросы субъектов ПДн, сроки их рассмотрения, а также типовые действия Оператора в ответ на обращения субъектов ПДн, их представителей.
2. Типовая форма бланка запроса субъекта ПДн на получение информации о его ПДн.
3. Типовая форма бланка отзыва согласия на обработку ПДн субъекта ПДн.
4. Типовая форма бланка запроса на блокирование (удаление), уточнение ПДн.

Специалист по защите информации М.О. Урутин

Приложение № 1
к Политике

Типовые запросы субъектов ПДн,
сроки их рассмотрения, а также типовые действия Оператора
в ответ на обращения субъектов ПДн, их представителей

Обращение (запрос)	Действия	Срок	Результат (ответ)
Обращение субъекта ПДн или его представителя			
Наличие ПДн	Подтверждение обработки ПДн	30 дней (согласно ч. 1 ст. 20, 152-ФЗ)	Подтверждение обработки ПДн
	Отказ от подтверждения обработки ПДн	30 дней (согласно ч. 2 ст. 20, 152-ФЗ)	Уведомление об отказе подтверждения обработки ПДн
Ознакомление с ПДн	Предоставление информации по ПДн	30 дней (согласно ч. 1 ст. 20, 152-ФЗ)	Подтверждение обработки ПДн, правовые основания и цели такой обработки
			Способы обработки ПДн
			Сведения о лицах, которые имеют доступ к ПДн
			Перечень обрабатываемых ПДн и источник их получения
			Сроки обработки ПДн, в том числе сроки их хранения
			Информация об осуществленной или о предполагаемой трансграничной передаче ПДн
	Отказ от предоставления информации по ПДн	30 дней (согласно ч. 2 ст. 20, 152-ФЗ)	Уведомление об отказе предоставления информации по ПДн
Уточнение ПДн	Изменение ПДн	7 рабочих дней со дня предоставления уточняющих сведений (согласно ч. 3 ст. 20, 152-ФЗ)	Уведомление о внесенных изменениях ПДн

Обращение (запрос)	Действия	Срок	Результат (ответ)
	Отказ от изменения ПДн	30 дней (согласно ч. 2 ст. 20, 152-ФЗ)	Уведомление об отказе изменений ПДн
Уничтожение ПДн	Уничтожение ПДн	7 рабочих дней со дня предоставления сведений о незаконном получении ПДн или отсутствии необходимости ПДн для заявленной цели обработки (согласно ч. 3 ст. 20 152-ФЗ)	Уведомление об уничтожении ПДн
	Отказ от уничтожения ПДн	30 дней (согласно ч. 2 ст. 20, 152-ФЗ)	Уведомление об отказе уничтожения ПДн
Отзыв согласия на обработку ПДн	Прекращение обработки и уничтожение ПДн	30 дней (согласно ч. 5 ст. 21, 152-ФЗ)	Уведомление о прекращении обработки и уничтожении ПДн
	Отказ от прекращения обработки и уничтожения ПДн	30 дней (согласно ч. 2 ст. 20, 152-ФЗ)	Уведомление об отказе прекращения обработки и уничтожения ПДн
Недостовер-ность ПДн субъекта	Блокировка ПДн	С момента обращения субъекта ПДн о недостоверности его ПДн или с момента получения запроса на период проверки (согласно ч. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях ПДн
	Изменение ПДн	7 рабочих дней со дня предоставления уточненных сведений (согласно ч. 2 ст. 21, 152-ФЗ)	
	Снятие блокировки ПДн		

Обращение (запрос)	Действия	Срок	Результат (ответ)
	Отказ изменения ПДн	30 дней (согласно ч. 2 ст. 20, 152-ФЗ)	Уведомление об отказе изменения ПДн
Неправомерность действий с ПДн субъекта	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно ч. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
	Уничтожение ПДн в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно ч. 3 ст. 21, 152-ФЗ)	Уведомление об уничтожении ПДн
Достижение цели обработки ПДн субъекта	Прекращение обработки ПДн	30 дней (согласно ч. 4 ст. 21, 152-ФЗ)	Уведомление об уничтожении ПДн
	Уничтожение ПДн		
Запрос Уполномоченного органа по защите прав субъектов ПДн			
Информация для Осуществления деятельности уполномоченного органа	Предоставление затребованной информации по ПДн	30 дней (согласно ч. 4 ст. 20, 152-ФЗ)	Предоставление затребованной информации по ПДн

Приложение № 2
к Политике

Запрос субъекта ПДн на получение информации о его ПДн

_____
(кому)
От _____,
_____ серия _____ № _____,
(документ, удостоверяющий личность)
выдан _____
_____,
(когда, кем)
проживающего по адресу_____
_____.

На основании своих законных прав субъекта персональных данных, прошу предоставить следующие сведения (выделить нужное):

подтверждение факта обработки моих персональных данных оператором ГАУ РО «ОКДЦ»;

правовые основания и цели обработки моих персональных данных;

цели и применяемые оператором ГАУ РО «ОКДЦ» способы обработки моих персональных данных;

наименование и место нахождения ГАУ РО «ОКДЦ», сведения о лицах (за исключением работников ГАУ РО «ОКДЦ»), которые имеют доступ к моим персональным данным;

мои обрабатываемые персональные данные, источник их получения;

сроки обработки моих персональных данных, в том числе сроки их хранения;

порядок осуществления моих прав, предусмотренных Федеральным законом о персональных данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку моих персональных данных по поручению ГАУ РО «ОКДЦ»;

иные сведения, предусмотренные законодательством Российской Федерации:

_____
_____
_____

Ответ прошу направить почтовым сообщением на указанный мною адрес.

«____» _____ 20___г. _____
(дата) (подпись) (ФИО)

Приложение № 3
к Политике

Отзыв согласия на обработку ПДн субъекта ПДн

_____
(кому)
От _____,
_____ серия _____ № _____,
(документ, удостоверяющий личность)
выдан _____
_____,
(когда, кем)
проживающего по адресу_____
_____.

Прошу Вас прекратить обработку моих персональных данных в связи с _____ _____
_____
_____.
(указать причину)

«____» _____ 20___г. _____
(дата) (подпись) (ФИО)

Приложение № 4
к Политике

Запрос на блокирование (удаление), уточнение персональных данных

_____
(кому)
От _____,
_____ серия _____ № _____,
(документ, удостоверяющий личность)
выдан _____
_____,
(когда, кем)
проживающего по адресу_____
_____.

Прошу (нужное выделить) блокировать, удалить, уточнить мои персональные данные по следующим причинам (нужное выделить):

персональные данные являются неполными;

персональные данные являются устаревшими;

персональные данные являются недостоверными;

персональные данные являются незаконно полученными;

персональные данные не являются необходимыми для заявленной цели обработки;

другое:_____
_____
_____.

«____» _____ 20___г. _____
(дата) (подпись) (ФИО)

Приложение № 2
к приказу ГАУ РО «ОКДЦ»
№ 301 от «01» июля 2025 г.

Перечень документов
определяющий порядок обработки персональных данных в ГАУ РО «ОКДЦ»

1. Положение о порядке работы с конфиденциальной информацией в государственном автономном учреждении Ростовской области «Областной консультативно-диагностический центр».

2. Политика обработки персональных данных в государственном автономном учреждении Ростовской области «Областной консультативно-диагностический центр».

3. Положение о разрешительной системе допуска к ИСПДн государственного автономного учреждения Ростовской области «Областной консультативно-диагностический центр».

4. Положение об организации и обеспечению защиты персональных данных в государственном автономном учреждении Ростовской области «Областной консультативно-диагностический центр» при их обработке в информационных системах персональных данных и/или без использования средств автоматизации.

5. Правила рассмотрения запросов субъектов персональных данных или их представителей в государственном автономном учреждении Ростовской области «Областной консультативно-диагностический центр».

6.Правила работы с обезличенными данными в случае обезличивания персональных данных в Государственном автономном учреждении Ростовской области «Областной консультативно-диагностический центр».

7. Правила осуществления внутреннего контроля соответствия обработки защищаемой информации, в том числе персональных данных, требованиям безопасности информации, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами в государственном автономном учреждении Ростовской области «Областной консультативно-диагностический центр».

8. Порядок учета, хранения и уничтожения машинных носителей персональных данных в ИСПДН государственного автономного учреждения Ростовской области «Областной консультативно-диагностический центр».

9. Сборник инструкций по порядку обращения с персональными данными в государственном автономном учреждении Ростовской области «Областной консультативно-диагностический центр».

10. Согласие на обработку персональных данных пациента.

11. Согласие на обработку персональных данных сотрудника.

12. Соглашение о неразглашении информации, содержащей персональные данные.

13. Ответственность за несоблюдение требований законодательства РФ в сфере защиты персональных данных.

Специалист по защите информации М.О. Урутин

Приложение №3
к приказу ГАУ РО «ОКДЦ»
№ 301 от «01» июля 2025 г.

ПОЛОЖЕНИЕ
о порядке работы с конфиденциальной информацией в ГАУ РО «ОКДЦ»

1. Общие положения

1.1. Настоящее Положение о порядке обработки персональных данных в ГАУ РО «ОКДЦ» (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Федеральными законами от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящее Положение является локальным нормативным актом, разработанным и утвержденным в целях обеспечения правовой и экономической безопасности ГАУ РО «ОКДЦ» (далее – Центр, Оператор), обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, защиты прав на неприкосновенность частной жизни, личной и семейной тайн, в том числе при проведении клинической лабораторной диагностики.

1.3. Настоящее Положение устанавливает порядок обращения с конфиденциальной информацией. Положение определяет цели, принципы, порядок и условия обработки конфиденциальной информации, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности этих данных при их обработке в информационных системах Центра.

1.4. Положение распространяются на все отношения, связанные с обработкой конфиденциальной информации, осуществляемой в Центре, в том числе при проведении клинической лабораторной диагностики.

Положение вступает в силу с момента его утверждения главным врачом Центра.

1.5. Положение подлежит пересмотру в ходе периодического анализа со стороны руководства Центра, а также в случаях изменения законодательства Российской Федерации в области обеспечения

безопасности конфиденциальной информации персональных данных.

1.6. Целью настоящего Положения является обеспечение безопасности конфиденциальной информации в Центре, в том числе содержащейся в информационных системах Центра.

1.7. Положение является общедоступным документом, декларирующим концептуальные основы деятельности Центра при обработке конфиденциальной информации.

1.8. Положение применяется ко всем сотрудникам Центра и субъектам персональных данных, которым оказываются медицинские услуги в Центре.

1.9. Основные понятия, используемые в Положении:

конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Информация, требующая защиты.

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

разглашение информации – несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации;

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

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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 информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

предоставление персональных данных – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному 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;

врачебная тайна – информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении;

коммерческая тайна – информация, позволяющая её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и которые обладатель таких сведений относит к коммерческой тайне.

2. Сведения, относимые к конфиденциальной информации

В соответствии с Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» в Центре к сведениям конфиденциальной характера относятся:

2.1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2.2. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная тайна).

2.3. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

3. Порядок допуска к конфиденциальной информации, документам и его прекращение

3.1. Основанием для допуска работников к конфиденциальной информации является подписание с ними трудового договора и включения

их в приказ о допуске к сведениям, составляющим конфиденциальную информацию.

3.2. До издания приказа о приёме на работу с кандидатом оформляется соглашение о неразглашении информации, содержащей конфиденциальную информацию, которое хранится в Центре.

3.3. После издания приказа о приёме на работу и до предоставления фактического доступа работника к сведениям, составляющим конфиденциальную информацию, руководитель структурного подразделения, в которое принимается работник:

доводит до работника под подпись настоящие нормативные правовые документы, регламентирующие порядок работы с конфиденциальной информацией (приложение №1);

предупреждает об ответственности за нарушение требований конфиденциальности информации;

3.4. Доступ работника к информационным ресурсам информационных систем Центра обеспечивается отделом информационных технологий и систем.

3.5. Фактический доступ работника к документам, машинным носителям и информационным ресурсам информационных систем Центра, содержащих конфиденциальную информацию, в объеме, необходимом для исполнения им должностных обязанностей, организует его непосредственный руководитель.

Руководители структурных подразделений несут персональную ответственность за выполнение требований по защите конфиденциальной информации работниками своего подразделения, допущенных к конфиденциальной информации, и обязаны обеспечить систематический контроль над тем, чтобы к указанной информации получали доступ только те лица, которым она необходима для выполнения своих должностных обязанностей.

3.6. Основанием для прекращения доступа к сведениям, составляющим конфиденциальную информацию, является:

приказ об увольнении работника;

заявление работника об увольнении, либо объявление работнику в соответствии с трудовым законодательством о предстоящем увольнении (в этом случае необходимость и объем работы с конфиденциальной информацией на период до издания приказа определяет руководитель структурного подразделения);

нарушение работником взятых на себя обязательств, связанных с неразглашением конфиденциальной информации;

решение главного врача об отстранении работника от работы со сведениями, составляющими конфиденциальную информацию. Решение оформляется приказом и доводится до сведения работника под подпись.

3.7. При увольнении работника, имеющего доступ к конфиденциальной информации, отстранении работника от работы со сведениями, составляющими конфиденциальную информацию, документы и иные носители, содержащие конфиденциальную информацию,

сдаются работником в отдел по гражданской обороне и мобилизационной работе специалисту по защите информации.

3.8. Командированные сторонними организациями лица допускаются к конфиденциальной информации Центра на основе письменного разрешения главного врача при наличии соглашения о конфиденциальности между Центром и командирующей организацией, письменного запроса руководителя организации, в которой работают командированные лица, с указанием целей получения конфиденциальной информации и перечня конкретных сведений.

4. Обязанности лиц, допущенных к конфиденциальной информации

4.1. Лица, допущенные к конфиденциальной информации обязаны:

знать и выполнять требования Положения и других нормативных правовых документов Центра, регламентирующих вопросы обеспечения конфиденциальности информации и порядка обращения с конфиденциальной информацией, в том числе при проведении клинической лабораторной диагностики;

соблюдать права пациентов при проведении клинической лабораторной диагностики;

соблюдать установленные в Центре правила работы с документами, порядок их учета, хранения и уничтожения;

знакомиться только с теми документами и информацией, к которым получен допуск в пределах должностных обязанностей;

во время работы с документами, содержащими конфиденциальную информацию, принимать меры к исключению возможности ознакомления с ними других лиц, не имеющих к ним прямого отношения;

пресекать действия других лиц, которые могут привести к разглашению сведений, содержащих конфиденциальную информацию;

не разглашать конфиденциальную информацию Центра и (или) её контрагентов без их согласия, не использовать ее для собственных нужд в период действия трудового договора;

в рабочее время, а также при краткосрочном отсутствии на рабочем месте документы, содержащие конфиденциальную информацию, хранить в закрытом на замок шкафу (сейфе);

при выполнении работ с документами, содержащими конфиденциальную информацию, руководствоваться нормативными правовыми документами Центра по ведению конфиденциального делопроизводства;

немедленно информировать руководителя структурного подразделения и специалиста по защите информации о фактах утраты (недостачи) документов (отдельных листов), содержащих врачебную тайну, ключей от сейфов (шкафов), фактах обнаружения неучтенных конфиденциальных документов, а также о фактах необоснованного интереса к сведениям, составляющим конфиденциальную информацию, со стороны лиц, не имеющих прямого отношения к работе с ними;

при переводе по работе, убытии в отпуск, длительную командировку

(более 1 месяца) сдать документы, содержащие конфиденциальную информацию руководителю структурного подразделения;

возмещать причиненные убытки, если он виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с исполнением им трудовых обязанностей.

4.2. Лицам, допущенным к конфиденциальной информации запрещается:

вести переговоры по конфиденциальным вопросам по незащищенным линиям связи, записывать и передавать (по сетям передачи данных общего пользования, телефону, интернет и т.д.) конфиденциальную информацию;

производить без разрешения главного врача звукозаписи по конфиденциальным вопросам;

использовать конфиденциальную информацию в открытой служебной переписке, докладах и выступлениях, в открытых статьях и других материалах, предназначенных для общего опубликования;

сообщать какую-либо информацию о проводимых конфиденциальных работах при обращении по личным вопросам, с жалобами, просьбами и предложениями в государственные органы и общественные организации;

сообщать в письменных сообщениях, направляемых в другие организации по вопросам контрагентских отношений, данные о характере проводимых конфиденциальных работ;

производить без разрешения главного врача видео-, фото- и киносъемки в помещениях Центра, в которых производятся конфиденциальные работы или работы с конфиденциальными документами.

4.3. При обработке конфиденциальной информации в информационных системах Центра работники обязаны:

соблюдать правила разграничения доступа к охраняемой информации, неукоснительно выполнять требования нормативных правовых документов по организации доступа к информационным ресурсам, организации парольной и антивирусной защиты;

не разглашать свои индивидуальные пароли на доступ к компьютерным, сетевым и иным информационным ресурсам, выполнять требования администратора информационных систем по смене паролей, не использовать «простые» пароли, не оставлять в легкодоступных местах сведения с индивидуальными паролями;

принимать меры к исключению ознакомления посторонних лиц с конфиденциальной информацией, выводимой на экран дисплея;

не использовать (не загружать, не запускать и т.д.) для обработки конфиденциальной информации посторонние программные средства, не допущенные для применения в Центре;

при необходимости покинуть свое рабочее место провести стандартные процедуры выхода из системы и отключения компьютера (в рабочее время допускается инициализация экранной заставки, защищенной индивидуальным паролем, или блокировка доступа к компьютеру с использованием аппаратно-программных средств и электронных ключей, принятых для эксплуатации в Центре);

не допускать случаев передачи информации, составляющей

конфиденциальную информацию, по незащищенным каналам передачи данных, через сеть интернет и иные публичные сети (включая факс);

не допускать применения средств криптографической защиты и защиты от несанкционированного доступа не предусмотренных эксплуатационной (технической) документацией на информационные системы Центра;

в нерабочее время, а также при кратковременном отсутствии на рабочем месте хранить съемные машинные носители, содержащие конфиденциальные сведения, в закрытом на замок шкафу (сейфе);

немедленно информировать руководителя структурного подразделения о фактах или возможности несанкционированного доступа к информации в информационных системах Центра.

5. Порядок обработки информации, содержащей сведения конфиденциального характера

5.1. Оператор имеет право на использование конфиденциальной информации любыми не запрещенными законодательством Российской Федерации способами и принимает меры к ее охране и ограничению доступа к ней третьих лиц.

5.2. Не допускается разглашение сведений конфиденциального характера.

5.3. Обработка персональных данных работников Центра и субъектов персональных данных осуществляется в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказа Центра от «___» июня 2025 г. №___ «Об актуализации политики обработки персональных данных в ГАУ РО «ОКДЦ».

5.4. Обработка сведений, содержащих врачебную тайну осуществляется в соответствии с требованиями Федеральных законов от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации, приказа Центра от «___» июня 2025 г. №___ «Об актуализации политики обработки персональных данных в ГАУ РО «ОКДЦ».

5.5. Обработка сведений, содержащих коммерческую тайну осуществляется в соответствии с требованиями Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», приказа Центра от «___» июня 2025 г. №___ «Об актуализации политики обработки персональных данных в ГАУ РО «ОКДЦ».

6. Цели обработки конфиденциальной информации

6.1 Оператор обрабатывает персональные данные в целях:

оформления трудовых отношений;

ведения кадрового делопроизводства;

содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями;

обеспечения личной безопасности работников и субъектов персональных данных,

6.2. Оператор обрабатывает сведения, составляющие врачебную тайну

в целях:

оказания медицинских услуг, в том числе идентификации пациентов (заказчиков);

отработки информации, полученной в результате лабораторной диагностики;

отражения информации в медицинской документации;

предоставления сведений страховым компаниям (в случае оплаты ими оказываемых услуг).

6.3. Оператор обрабатывает сведения, составляющие коммерческую тайну в целях:

заключения, исполнения и прекращения гражданско-правовых договоров;

предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг;

учета сведений, связанных с предпринимательской деятельностью Центра по оказанию медицинских платных услуг населению;

в иных случаях, установленных Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» или указанных в Уставе Центра.

6.4. Обработка конфиденциальной информации должна осуществляться на основании требований федеральных законов и других нормативных правовых актов Российской Федерации.

6.5. Обработка конфиденциальной информации должна ограничиваться достижением конкретных, заранее определенных и законных целей.

6.6. Обрабатываемая конфиденциальная информация не должна быть избыточна по отношению к заявленным целям ее обработки.

7. Защита конфиденциальной информации при обработке информации в информационных системах Центра

7.1. Сохранность конфиденциальной информации при ее обработке на средствах вычислительной техники (далее — СВТ) и передаче информационных системах Центра обеспечивается осуществлением комплекса организационных, организационно-технических и программных мер защиты информации.

7.2. Обязательными условиями обработки конфиденциальной информации на СВТ являются:

персональный допуск пользователей к работе на СВТ в соответствии с установленным порядком;

разграничение полномочий и доступа пользователей к информационным ресурсам информационных систем Центра (обеспечивается системными средствами разграничения, использованием индивидуальных идентификаторов и паролей, электронных ключей и т.д.);

ведение учета всех электронных носителей конфиденциальной информации;

обособленное хранение (в отдельных областях сетевых дисков, директориях, папках, файлах и т.д.) сведений, составляющих

конфиденциальную информацию, с максимально возможным разграничением доступа к ней;

создание резервных копий информационных массивов;

стирание по истечению практической надобности информации и проектов документов, содержащих конфиденциальную информацию, оставшихся на внешних запоминающих устройствах СВТ;

уничтожение информации с машинных носителей (уничтожение машинных носителей информации), на которые осуществлялась запись конфиденциальной информации в случаях выхода их из строя или непригодности (нецелесообразности) для дальнейшего использования, а также при плановой или внеплановой замене СВТ;

ограничение работников Центра в записи информации на внешние носители информации в соответствии с матрицей доступа пользователей (CD-RW диски, флеш-накопители и т.д.);

организация обособленной установки серверного и коммуникационного оборудования в отдельных, специально выделенных, опечатываемых помещениях (серверных), которые должны находиться под постоянной охранной сигнализацией и вход в которые должен быть максимально ограничен;

регистрация печатных копий и электронных носителей документов, содержащих конфиденциальную информацию;

исключение несанкционированного доступа к информационным массивам, содержащим конфиденциальную информацию;

недопущение передачи сведений, составляющих конфиденциальную информацию по незащищенным каналам связи.

8. Требования по оборудованию помещений и рабочих мест

8.1. Входные двери помещений, в которых производится обработка и хранение документов, содержащих конфиденциальную информацию, должны быть оборудованы замками, гарантирующими надежное их закрытие.

8.2. Порядок использования ключей должен исключать несанкционированный доступ в эти помещения посторонних лиц.

8.3 Для хранения документов, содержащих конфиденциальную информацию, работники обеспечиваются запирающимися шкафами (сейфами), а также необходимым количеством папок для хранения документов, содержащих сведения конфиденциального характера.

8.4. Порядок опечатывания шкафов (сейфов), где хранятся сведения, содержащие конфиденциальную информацию, определяется руководителем структурного подразделения. Обязательному закрытию и опечатыванию подлежат запирающиеся шкафы (сейфы) с конфиденциальными документами, размещающиеся в общих коридорах.

8.5. По решению главного врача, помещения, предназначенные для ведения конфиденциальных переговоров, могут быть аттестованы на соответствие требованиям по безопасности информации.

8.6. Установка и замена оборудования, мебели, ремонт в аттестованных на соответствие требованиям по безопасности информации

помещениях должны производиться по согласованию с главным врачом и с осуществлением контроля со стороны специалиста по защите информации.

9. Порядок предоставления и передачи конфиденциальной информации сторонним организациям

9.1. Предоставление конфиденциальной информации о деятельности Центра органам государственной власти, иным государственным органам, органам местного самоуправления и контрагентам осуществляется в порядке, установленном законодательством Российской Федерации.

9.2. Передача сторонним организациям и физическим лицам конфиденциальной информации о контрагентах Центра должна осуществляться с письменного согласия последних на основании соответствующих запросов.

9.3. Передача конфиденциальной информации должна осуществляться на бумажных носителях, если их передача на иных носителях не предусмотрена действующим законодательством Российской Федерации.

9.4. В случае обоснованной необходимости передача конфиденциальных сведений на электронном носителе осуществляется сопроводительным письмом в соответствии с порядком, определенным в Центре. В сопроводительном письме указываются перечень и ограничительный гриф отдельных файлов (информационных массивов), записанных на данном носителе. Гриф, проставляемый на самом машинном носителе, должен быть не ниже высшего ограничительного грифа информации, на нем записанной.

9.5 Передача конфиденциальной информации сторонним организациям на электронных носителях, в том числе запись информации на электронные носители принимающей стороны, без разрешения главного врача или уполномоченных им лиц, запрещается.

10. Порядок доступа к конфиденциальной информации Центра работников сторонних организаций

10.1 Доступ командированных в Центр работников сторонних организаций к конфиденциальной информации и документам осуществляется решением главного врача в объеме, необходимом исключительно для выполнения задач командировки.

10.2. Доступ к ресурсам электронных информационных систем Центра осуществляется на основании заявки. Заявка подписывается главным врачом, руководителем соответствующего структурного подразделения, в которое прибыл командированный работник, и согласовывается с начальником отдела информационных технологий и систем.

10.3. Непосредственный доступ к ресурсам электронных информационных систем осуществляет отдел информационных технологий и систем.

10.4. В общем порядке доступ представителей сторонних организаций, а также физических лиц, оказывающих услуги (выполняющих работы) Центру к электронным источникам информации, запрещен.

10.4.1. К совершению отдельных операций с использованием информационных систем Центра представители сторонних организаций допускаются на основании письменного разрешения главного врача или лица, его замещающего.

10.4.2. Допуск представителей сторонних организаций к информации, содержащей сведения конфиденциального характера, для совершения отдельных операций с использованием информационных систем Центра, осуществляется на основании соответствующей заявки, в соответствии с требованиями норм действующего законодательства.

10.5. Контроль соблюдения представителями сторонних организаций требований конфиденциальности информации при использовании информационных систем Центра возлагается на руководителей структурных подразделений, к которым прибыли представители.

11.Ответственность за разглашение информации (сведений), составляющих конфиденциальную информацию

11.1. Каждый работник Центра, получающий для работы сведения или документы, содержащие конфиденциальную информацию, в том числе персональные данные работников и субъектов персональных данных, несет ответственность за сохранность носителя конфиденциальной информации и конфиденциальность информации.

11.2. Лица, виновные в нарушении норм, регулирующих порядок обращения с информацией, содержащей сведения конфиденциального характера Центра, в том числе получение, обработку и защиту персональных данных, несут дисциплинарную, материальную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством Российской Федерации.

12. Проведение служебного расследования по фактам разглашения (утраты) конфиденциальных сведений

12.1. По фактам разглашения (утраты) сведений, составляющих конфиденциальную информацию, проводится служебное расследование.

Служебное расследование может также назначаться по фактам грубого нарушения установленных нормативными документами правил обращения с конфиденциальной информацией.

Для проведения служебного расследования приказом Центра назначается комиссия в составе не менее трех человек.

Руководитель структурного подразделения всесторонне обеспечивает работу комиссии в подразделении, где выявлены факты разглашения (утраты) сведений, составляющих конфиденциальную информацию.

12.2. Комиссия, проводящая служебное расследование:

выясняет обстоятельства, причины разглашения сведений или утраты документов конфиденциального характера, а также способствовавшие этому условия;

устанавливает лиц, виновных в разглашении сведений или утрате документов конфиденциального характера;

принимает меры к розыску утраченного документа или

предотвращению негативных последствий разглашения сведений конфиденциального характера.

12.3. Члены комиссии, проводящие служебное расследование, имеют право:

производить осмотр помещений Центра, где обрабатывались сведения, конфиденциального характера (сейфов, столов, шкафов, и т.д.);

проверять конфиденциальную документацию, журналы учета конфиденциальных документов и другую документацию;

опрашивать работников Центра, допустивших утрату (разглашении) сведений, содержащих конфиденциальную информацию, а также других работников Центра, способных оказать содействие в установлении обстоятельств происшедшего и получать от них письменные объяснения;

привлекать работников других структурных подразделений Центра, не заинтересованных в исходе дела, для проведения отдельных действий служебного расследования по согласованию с их руководителями.

12.4. Служебное расследование проводится в минимально короткий срок, но не более 10 рабочих дней со дня назначения комиссии.

12.5. По результатам расследования составляется заключение, в котором отражаются следующие вопросы:

основания для проведения расследования;

состав комиссии и сроки проведения расследования;

перечень и результаты проведённых мероприятий;

выявленные виновные лица;

выявленные причины и условия, способствовавшие разглашению (утрате) сведений, составляющих конфиденциальную информацию;

возможные негативные последствия происшедшего для интересов Центра и предложения по их устранению;

вывод о наличии в действиях виновного лица признаков административного правонарушения, либо уголовно-наказуемого деяния.

12.6. Заключение по результатам служебного расследования докладывается главному врачу для принятия решения о привлечении виновного к дисциплинарной ответственности либо о передаче материалов в правоохранительные или судебные органы, а также о мерах по устранению причин и возможных негативных последствий происшедшего либо об отклонении материалов расследования.

13. Контроль состояния конфиденциальности информации

13.1. Общая организация контроля состояния конфиденциальности информации возлагается на главного врача, непосредственный контроль за выполнение требований по защите конфиденциальной информации – на специалиста по защите информации Центра.

13.2. Контроль состояния конфиденциальности информации в Центре осуществляется с целью определения соответствия принятых мер по защите конфиденциальной информации, выявления возможных каналов утечки и несанкционированного доступа к данной информации и принятию мер по их пресечению.

13.3. Контроль обеспечения сохранности сведений, составляющих

конфиденциальную информацию может осуществляться в форме:

повседневного контроля правил соблюдения требований по защите конфиденциальной информации (без составления акта);

ежегодных проверок правил соблюдения требований по защите конфиденциальной информации (с составлением акта);

плановой проверки в конкретном структурном подразделении Центра или на конкретном рабочем месте работника Центра;

внеплановой проверки по указанию главного врача.

13.4. В ходе проверки проводится:

оценка деятельности структурного подразделения Центра по защите конфиденциальной информации;

анализ состояния защищенности информационных ресурсов и технологий, подготовка предложений по совершенствованию их защиты;

выявление каналов утечки информации и несанкционированного доступа к информации;

анализ причин нарушений и недостатков в организации и обеспечении защиты информации в структурных подразделениях Центра, разработка рекомендаций по их устранению.

13.5 При выявлении в ходе проверки факта разглашения информации, составляющей конфиденциальную информацию, утраты документов или иных носителей информации, содержащих указанные сведения, в структурном подразделении проводится служебное расследование.

13.6. По результатам проверки составляется акт состояния конфиденциальности информации в Центре, выявленных недостатков и нарушений в ходе проверки, предложения по их устранению.

Специалист по защите информации М.О. Урутин