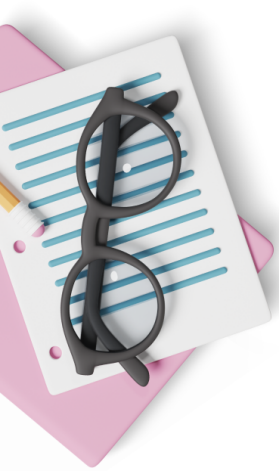
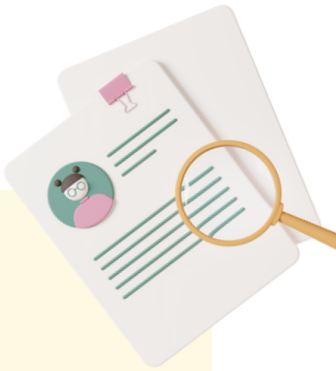
ЦОКО
ЦЕНТР ОЦЕНКИ КВАЛИФИКАЦИИ И ОБУЧЕНИЯ №1

COKO1.RU

Алгоритм организации работы с персональными данными в медоорганизациях



Назначьте ответственных за работу с персональными данными в медорганизации



Закон не устанавливает требований к работнику, который занимается обработкой персональных данных. Вы можете назначить ответственным сотрудника отдела кадров, специалиста информационно-технического отдела или заместителя главврача. Издайте приказ о назначении и поручите прописать обязанности в должностной инструкции.

Образец приказа о назначении ответственного по работе с персональными данными

ГБУЗ «Больница»

ПРИКАЗ

от 26 июля 2023 г. № 364

Об ответственном за организацию обработки персональных данных в ГБУЗ «Больница»

В целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»,

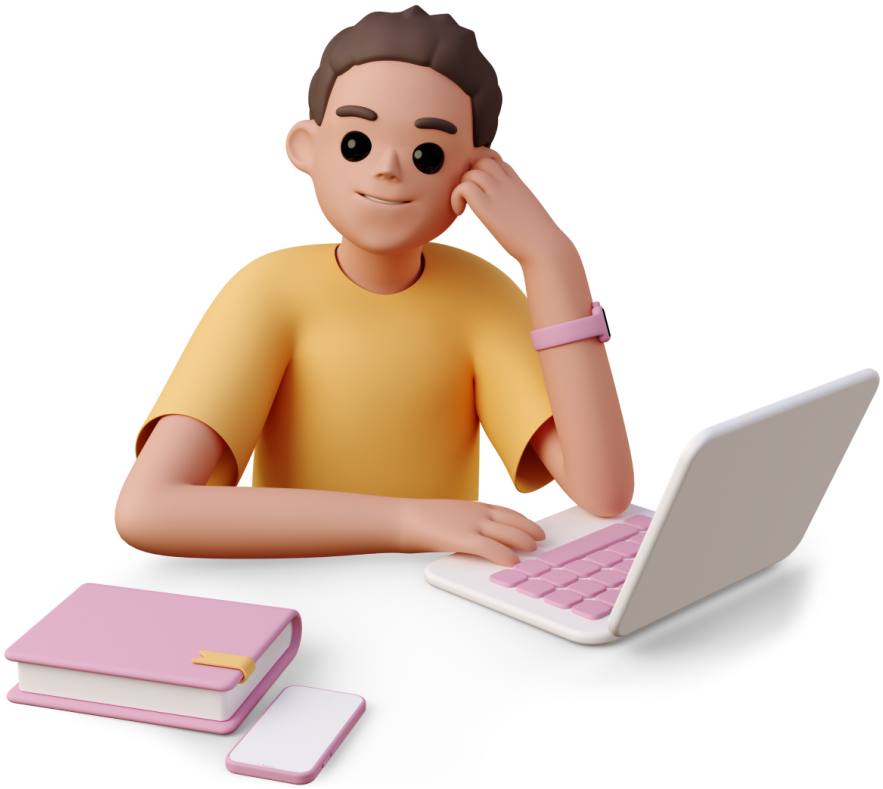
ПРИКАЗЫВАЮ:

1. Назначить заместителя главного врача по медицинской части Иванову И.И. ответственным за организацию обработки персональных данных в ГБУЗ «Больница».

2. Утвердить прилагаемую Инструкцию ответственного за организацию обработки персональных данных в ГБУЗ «Больница».

Нельзя назначить несколько ответственных за обработку персональных данных. Например, одного — за обработку личной информации сотрудников, другого — данных пациентов. Роскомнадзор за это штрафует. При этом официальных разъяснений, почему это запрещено, нет.

Нельзя назначить несколько ответственных за обработку персональных данных. Например, одного — за обработку личной информации сотрудников, другого — данных пациентов. Роскомнадзор за это штрафует. При этом официальных разъяснений, почему это запрещено, нет.



Разработайте положение о защите персональных данных

Поручите ответственному лицу разработать Положение о работе с персональными данными, Положение об обработке персданных и Положение о защите персданных сотрудников и пациентов.
В медорганизации должны быть все три документа. В них прописывайте только те категории информации, которые нужны для работы сотрудников или оказания медпомощи пациентам. Например, СНИЛС потребуется для отправки информации в СФР, а электронная почта пациента — для направления результатов анализов, телефон — для связи с лечащим врачом.

Для каждой цели обработки ПД определите:

- Категории и перечень данных
- Категории субъектов ПД
- Способы, сроки их обработки и хранения
- Порядок уничтожения информации при достижении целей ее обработки или при наступлении иных законных оснований

Образец Положения о работе с персональными данными сотрудников

Положение о работе с персональными данными

1. Общие положения

1.1. Положение о работе с персональными данными работников _____ разработано в соответствии с Трудовым кодексом РФ, Законом от 27.07.2006 № 152-ФЗ и нормативно-правовыми актами, действующими на территории РФ.

1.2. Настоящее Положение определяет порядок работы (сбора, обработки, использования, хранения и т. д.) с персональными данными работников и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю.

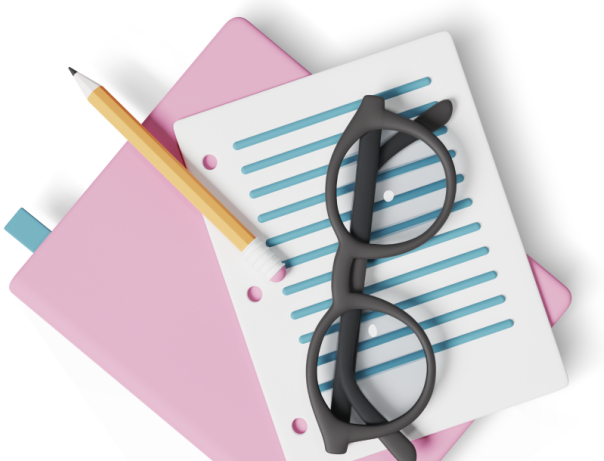
1.3. Настоящее Положение вступает в силу с _____.

2. Получение и обработка персональных данных работников

2.1. Персональные данные работника работодатель получает непосредственно от работника. Работодатель вправе получать персональные данные работника от третьих лиц только при наличии письменного согласия работника или в иных случаях, прямо предусмотренных в законодательстве.

2.2. При поступлении на работу работник заполняет анкету, в которой указывает следующие сведения о себе:
– пол;
– дату рождения;
– семейное положение;

Все параметры обработки и защиты персданных работников и пациентов прописывайте отдельно. Единственное, что можно объединить — правила защиты личной информации сотрудников и пациентов. Для этого достаточно одного Положения.



Создайте комиссию по персданным

Возглавлять комиссию может главный врач, директор клиники или лицо, которое отвечает в медицинском учреждении за персданные. Утвердите состав комиссии приказом. При необходимости пропишите обязанности в допсоглашениях к трудовым договорам.

Образец приказа о создании комиссии по установлению уровня защищенности персональных данных

ГБУЗ БОЛЬНИЦА

ПРИКАЗ

от 11.01.2023 **№ *** - п**

О создании комиссии по установлению уровня защищенности персональных данных в информационных системах персональных данных ГБУЗ БОЛЬНИЦА

В соответствии со статьей 18.1 Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных" п р и к а з ы в а ю:

1. Назначить комиссию по установлению уровня защищенности персональных данных в информационных системах персональных данных в составе:

ФИО	-	Заместитель главного врача по медицинской части, председатель комиссии;
ФИО	-	Специалист информационно-технического отдела;

Поручите членам комиссии установить уровень защищенности персональных данных в информационных системах медорганизации и разработать комплекс защищающих мероприятий. Пусть они опираются на Постановление Правительства от 01.11.2012 № 1119.

Чтобы разработать систему защиты ПД, комиссия, назначенная главврачом, должна:

- Обследовать информационную систему персональных данных (ИСПД);
- Выделить подсистемы, где обрабатываются данные
- Определить категорию обрабатываемых данных, их объем, например, специальные, биометрические, общедоступные
- На основании анализа присвоить информационной системе один из четырех классов безопасности — К1, К2, К3, К4.

Комиссия может привлекать для анализа системы экспертов — лицензиатов Федеральной службы по техническому и экспортному контролю. Перечень экспертных организаций есть в реестре ФСТЭК. По итогам члены комиссии должны подписать акт, классифицирующий персданные.

Составьте матрицу доступа к личным данным

Матрица нужна для того, чтобы распределять ответственность сотрудников за информационную безопасность. Поручите ведение матрицы доступа службе информационной безопасности.
Так как законодательно утвержденной матрицы доступа нет, ее можно заполнять в произвольном виде.

Образец матрицы уровней доступа к личным данным сотрудников

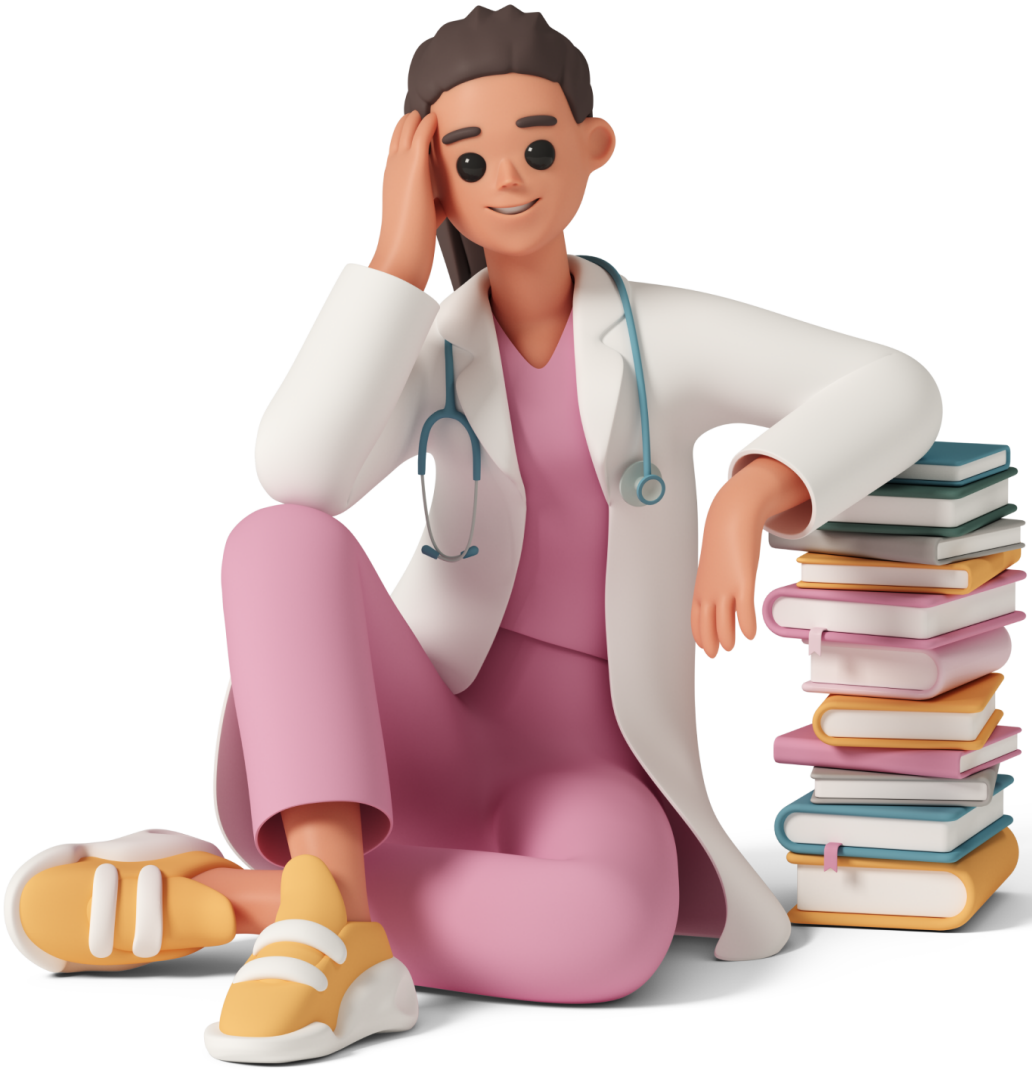
Должность	Полномочия	Примечание
Главный врач	Чтение	Контроль
Ответственный за информационную безопасность	Полный доступ ко всем техническим средствам обработки информации и данным ИСПДн	Контроль
Главный бухгалтер	Чтение	Контроль
Заместитель главного врача по кадрам	Обработка ПД (п. 3 ст. 3 Федерального закона «О персональных данных»)	Оформление трудовых отношений
Заведующие отделениями	Чтение	Только дела своих подчиненных
Сотрудники МО	Чтение	Только свои личные дела

Создайте условия о хранении персональных данных

Определите места хранения бумажных документов. Например, медорганизация должна хранить в специальном кабинете:

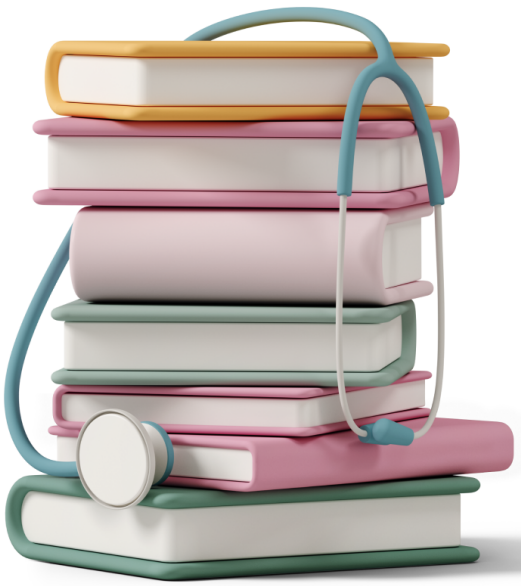
Карты пациентов, выбывших из стационара

Ксерокопии паспортов и полисов, которые необходимы для оформления счетов-фактур и реестров по ОМС



Чтобы избежать утечки информации, определите перечень лиц, которые вправе работать с данными, а также вести журнал доступа. Разрешите доступ к документам регистраторам приемного отделения, врачам-статистики, операторам (по ОМС), заместителю главврача. Храните материальные носители так, чтобы обеспечить сохранность персональных данных и исключить несанкционированный к ним доступ. Вы или члены комиссии можете самостоятельно определить перечень мер, которые позволят сохранить и защитить информацию. Такие правила установлены в п. 13-15 Постановления Правительства РФ от 15 сентября 2008 г. № 687.

Если в медорганизации обрабатываются персональные данные в информационной системе, то обеспечивайте ее защиту от несанкционированного доступа, чтобы исполнить требования Постановления Правительства РФ от 1 ноября 2012 г. № 1119. Выдайте ключи доступа к данным только тем, кто работает с информацией.



ЦОКО

ЦЕНТР ОЦЕНКИ КВАЛИФИКАЦИИ И ОБУЧЕНИЯ №1

COKO1.RU

Центр оценки квалификации и обучения №1

Повышение квалификации, профессиональная переподготовка и аккредитация для высшего и среднего медицинского персонала

- 400+ программ и направлений
- Помогаем успешно пройти аккредитацию медицинскому персоналу
- Предоставляем рассрочку и скидки для групп
- Курсы, семинары и лекции с баллами НМО
- Дистанционный формат обучения
- Учебные программы соответствуют профессиональным стандартам и ФГОС
- Поддержка в обучении от старта и до выдачи документов