УТВЕРЖДАЮ
Генеральный директор
ООО «Клиника на Кутузовском»
Лебедев О.В.

«20» мая 2025 г.

ПРАВИЛА ВНУТРЕННЕГО КОНТРОЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ООО «Клиника на Кутузовском»

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Постановлением Правительства РФ № 1119, № 687, Приказом ФСТЭК № 21, а также иными нормативными актами, регулирующими обработку и защиту персональных данных (далее – ПДн).

1.2. Целью настоящих Правил является обеспечение защиты прав и законных интересов субъектов персональных данных, а также соблюдение требований законодательства при их обработке в ООО «Клиника на Кутузовском».

1.3. Настоящие Правила обязательны для исполнения всеми сотрудниками ООО «Клиника на Кутузовском», участвующими в обработке ПДн.

1.4. Контроль за исполнением настоящих Правил возлагается на Ответственного за организацию обработки персональных данных, назначенного приказом Генерального директора ООО «Клиника на Кутузовском».

2. Принципы обработки персональных данных

2.1. Обработка ПДн осуществляется на законной и справедливой основе.

2.2. Цели обработки ПДн должны быть заранее определены и законны.

2.3. Объем и содержание обрабатываемых ПДн должны соответствовать заявленным целям их обработки, исключая избыточность.

2.4. Хранение ПДн осуществляется не дольше установленного срока, необходимого для достижения целей обработки.

2.5. Обеспечивается конфиденциальность персональных данных, исключая их распространение без согласия субъекта или на основании закона.

3. Цели обработки персональных данных

3.1. Для пациентов:

- Оказание медицинских услуг, ведение медицинской документации, контроль качества лечения;

- Взаимодействие со страховыми организациями по ОМС и ДМС;
- Выполнение требований законодательства в области здравоохранения.

3.2. Для сотрудников:

- Кадровый учет, расчет заработной платы, обеспечение социальных гарантий;
- Соблюдение требований трудового законодательства РФ.

3.3. Для контрагентов:

- Исполнение договорных обязательств, учет и контроль взаимодействий.

4. Порядок внутреннего контроля за обработкой ПДн

4.1. Внутренний контроль осуществляется в следующих формах:

- Плановые проверки (не реже одного раза в год);
- Внеплановые проверки (в случае инцидентов или запросов Роскомнадзора).

4.2. Ответственный за внутренний контроль обязан:

- Проверять соблюдение сотрудниками требований законодательства и локальных актов ООО «Клиника на Кутузовском» в части обработки ПДн;
- Проводить аудит эффективности мер защиты ПДн;
- Готовить отчеты о результатах проверки и предлагать меры по устранению выявленных нарушений.

4.3. Результаты проверок оформляются в виде актов и представляются Генеральному директору.

5. Меры по обеспечению безопасности персональных данных

5.1. ООО «Клиника на Кутузовском» реализует следующие меры:

- Назначение Ответственного за обработку персональных данных;
- Ведение журналов учета доступа к ПДн, уничтожения ПДн, регистрации действий в ИСПДн;
- Использование сертифицированных средств защиты информации (антивирусного ПО, межсетевых экранов);
- Ограничение доступа к ПДн на основании должностных обязанностей сотрудников;
- Проведение регулярного обучения сотрудников по вопросам обработки и защиты ПДн.

5.2. Уровень защиты ИСПДн соответствует требованиям Постановления Правительства РФ № 1119.

6. Права субъектов персональных данных

6.1. Субъекты ПДн имеют право:

- Получать информацию об обработке их данных;
- Требовать уточнения, блокирования или уничтожения своих ПДн;

- Отозвать согласие на обработку ПДн, за исключением случаев, предусмотренных законодательством.

6.2. Запросы субъектов обрабатываются в срок не более 30 календарных дней.

7. Порядок обработки персональных данных

7.1. Обработка ПДн осуществляется с согласия субъекта, за исключением случаев, предусмотренных законом.

7.2. Согласие на обработку ПДн включает:

- Цели обработки;
- Перечень обрабатываемых данных;
- Срок хранения данных;
- Порядок отзыва согласия.

7.3. Обработка ПДн без автоматизации осуществляется в соответствии с ПП РФ № 687.

8. Ответственность за нарушение правил обработки ПДн

8.1. Лица, виновные в нарушении настоящих Правил, привлекаются к дисциплинарной, административной, гражданской или уголовной ответственности в соответствии с законодательством РФ.

8.2. ООО «Клиника на Кутузовском» несет ответственность за утрату и неправомерное использование ПДн.

9. Заключительные положения

9.1. Настоящие Правила вступают в силу с момента их утверждения Генеральным директором ООО «Клиника на Кутузовском».

9.2. Контроль за исполнением настоящих Правил возлагается на Ответственного за организацию обработки персональных данных.