**ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**в ООО "МИРАДА"**
(ИНН 7810197679, ОГРН 1037821035119)

**УТВЕРЖДАЮ**
Генеральный директор
ООО "МИРАДА"

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ № 1119 от 01.11.2012, и иными нормативными актами РФ.
1.2. Цель документа: установление порядка обработки и защиты ПДн в ООО "МИРАДА" (далее – «Оператор»).
1.3. Действие Положения распространяется на всех сотрудников Оператора, обрабатывающих ПДн.

**2. ОПРЕДЕЛЕНИЯ**

* **Персональные данные (ПДн):** Любая информация, относящаяся к прямо/косвенно определенному физлицу.
* **Субъект ПДн:** Пациент, сотрудник, контрагент или посетитель сайта mirada-med.ru.
* **Обработка ПДн:** Любые действия с ПДн (сбор, хранение, передача, обезличивание, уничтожение).
* **Оператор:** ООО "МИРАДА".

**3. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Обрабатываются категории ПДн:

* **Пациенты:** ФИО, паспортные данные, СНИЛС, полис ОМС/ДМС, адрес, телефон, e-mail, сведения о здоровье (диагнозы, назначения, результаты обследований).
* **Сотрудники:** Данные трудовых договоров, документов удостоверения личности, ИНН, СНИЛС, воинский учет.
* **Пользователи сайта:** Данные из форм обратной связи/записи (ФИО, телефон, e-mail), cookie.

**4. ЦЕЛИ ОБРАБОТКИ**

4.1. Для пациентов:

* Заключение и исполнение договоров на медуслуги;
* Ведение медицинской документации;
* Взаимодействие со страховыми компаниями.
4.2. Для сотрудников:
* Исполнение трудовых договоров;
* Начисление зарплаты;
* Отчетность перед госорганами.
4.3. Для пользователей сайта:
* Обработка запросов и записей на прием;
* Информирование об услугах (с согласия).

**5. ПРАВОВЫЕ ОСНОВАНИЯ**

* Согласие субъекта ПДн;
* Исполнение договора (оказание медуслуг, трудовой договор);
* Выполнение требований законодательства (ФЗ-152, ФЗ-323, НК РФ).

**6. МЕРЫ ЗАЩИТЫ ПДн**

6.1. **Организационные:**

* Назначение ответственного за обработку ПДн (приказом);
* Регулярное обучение сотрудников;
* Локальные акты: «Инструкция ответственного за ПДн», «Порядок резервного копирования».
6.2. **Технические:**
* Средства криптозащиты (СКЗИ);
* Антивирусная защита;
* Межсетевые экраны;
* Разграничение прав доступа к информационным системам;
* Хранение бумажных носителей в сейфах.

**7. ПЕРЕДАЧА ПДн ТРЕТЬИМ ЛИЦАМ**

Передача допускается только:

* В страховые компании (для ДМС/ОМС);
* В государственные органы (по запросам Росздравнадзора, ФНС);
* В лаборатории/партнерские клиники (только с письменного согласия пациента).

**8. ПРАВА СУБЪЕКТОВ ПДн**

Субъект ПДн вправе:

* Требовать доступ к своим ПДн;
* Уточнять, блокировать или уничтожать ПДн;
* Отозвать согласие на обработку;

**9. СРОКИ ХРАНЕНИЯ**

| **Категория ПДн** | **Срок хранения** |
| --- | --- |
| Медицинские данные | Не менее 5 лет (ст. 17 ФЗ-323) |
| Данные сотрудников | 50/75 лет (ст. 22.1 ТК РФ) |
| Данные пользователей | До отзыва согласия или 5 лет |

**10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

10.1. Контроль исполнения Положения осуществляет ответственный за обработку ПДн.
10.2. Изменения в Положение вносятся приказом Генерального директора.
10.3. Нарушение требований Положения влечет дисциплинарную, материальную или уголовную ответственность.