Методические рекомендации

по обеспечению защищённого обмена медицинскими персональными данными

между медицинской организацией и **ООО «ЭлНетМед»**

---

1. Общие положения

1.1. Цель документа

Обеспечение **законного, защищённого и контролируемого обмена медицинскими персональными данными (МПДн)** между:

1. **Медицинской организацией**, использующей медицинскую информационную систему (МИС), установленную на рабочих станциях, подключённых к корпоративной сети передачи данных **Министерства здравоохранения Алтайского края**.
2. **ООО «ЭлНетМед»**, обладающим собственной защищённой и аттестованной информационной инфраструктурой.

Обмен осуществляется **через защищённое соединение ViPNet** с выделенного автоматизированного рабочего места (АРМ).

---

2. Нормативно-правовая база РФ (обязательная)

2.1. Федеральное законодательство

Обмен и обработка МПДн должны соответствовать:

- **ФЗ №152-ФЗ** «О персональных данных»
- **ФЗ №323-ФЗ** «Об основах охраны здоровья граждан»
- **ФЗ №149-ФЗ** «Об информации, информационных технологиях и о защите информации»
- **ФЗ №187-ФЗ** (при наличии признаков КИИ)

2.2. Подзаконные акты и приказы

- Постановление Правительства РФ №1119 — уровни защищённости ПДн
- Приказ ФСТЭК №21 — организационные и технические меры защиты
- Приказ ФСБ №378 — криптографическая защита
- Приказ Минздрава РФ №965н — требования к МИС и защите медданных

---

3. Роли и ответственность сторон

3.1. Медицинская организация

- **Оператор персональных данных**
- Ответственна за:
    - законность передачи данных;
    - минимизацию объёма передаваемых МПДн;
    - идентификацию и аутентификацию пользователей;
    - защиту АРМ, с которого осуществляется обмен.

3.2. ООО «ЭлНетМед»

- **Обработчик персональных данных**
- Обязано:
    - обрабатывать МПДн строго по поручению оператора;
    - использовать аттестованную ИСПДн;
    - обеспечивать криптографическую защиту и аудит доступа.

---

4. Классификация информации и ИСПДн

4.1. Категория данных

- **Специальная категория ПДн** (сведения о состоянии здоровья)

4.2. Уровень защищённости

Рекомендуется:

- **Уровень защищённости ИСПДн — не ниже УЗ-1 или УЗ-2**
  (в зависимости от масштабов и угроз)

---

5. Организационные мероприятия (обязательные)

5.1. Документирование

В медицинской организации должны быть утверждены:

- Политика обработки ПДн
- Модель угроз безопасности информации
- Положение об ИСПДн
- Перечень лиц, допущенных к МПДн
- Регламент взаимодействия с ООО «ЭлНетМед»
- Согласие пациентов или законное основание передачи данных

5.2. Договорные меры

Обязательно наличие:

- **Договора поручения на обработку ПДн** с ООО «ЭлНетМед»
- SLA / регламента обмена
- Обязательств о неразглашении (NDA)

---

6. Технические мероприятия (ключевой раздел)

6.1. Выделенный АРМ для обмена

Обмен допускается **только**:

- с выделенного компьютера;
- включённого в домен/сегмент медорганизации;
- с установленным и настроенным **клиентом ViPNet**.

❗ Запрещается использовать личные или неаттестованные рабочие станции.

6.2. Сетевая сегментация

- АРМ обмена должен находиться:
  - либо в отдельной VLAN;
  - либо в выделенном сегменте ЛВС.
- Ограничение сетевых взаимодействий по принципу **deny by default**.

6.3. Криптографическая защита (ViPNet)

Обязательно:

- Использование **сертифицированных СКЗИ ViPNet**
- Настройка:
  - шифрования каналов связи;
  - аутентификации по ключам;
  - доверенных узлов ООО «ЭлНетМед».
- Хранение ключей:
  - в защищённом контейнере;
  - с разграничением доступа.

6.4. Защита АРМ

На компьютере обмена должны быть:

- сертифицированный антивирус;
- СЗИ НСД (при необходимости);
- актуальные обновления ОС;
- запрет USB-накопителей (или контроль);
- журналирование событий ИБ.

---

7. Управление доступом

7.1. Пользователи

- Персонифицированные учётные записи
- Запрет общих логинов
- Многофакторная аутентификация (рекомендуется)

7.2. Права доступа

- Минимально необходимые полномочия
- Разграничение:
    - просмотра;
    - передачи;
    - администрирования.

---

8. Контроль, аудит и реагирование

8.1. Журналирование

Фиксируются:

- факты подключения ViPNet;
- передача файлов/запросов;
- ошибки и попытки НСД.

8.2. Инциденты ИБ

Должен быть регламент:

- выявления;
- регистрации;
- уведомления;
- расследования инцидентов.

9. Аттестация и соответствие требованиям

9.1. ООО «ЭлНетМед»

- Аттестованная ИСПДн (ФСТЭК)
- Сертифицированные СКЗИ

9.2. Медицинская организация

- Локальная оценка соответствия
- При необходимости — аттестация АРМ обмена как части ИСПДн

---

10. Минимально достаточная архитектура (рекомендация)

МИС → Выделенный АРМ → ViPNet (ГОСТ) → Защищённая сеть ООО «ЭлНетМед»

Без прямого выхода МИС во внешние сети.

---

11. Итоговый вывод

Предложенный комплекс мероприятий является:

- **необходимым** — для соблюдения ФЗ-152 и ФЗ-323;
- **достаточным** — при использовании ViPNet и аттестованной ИСПДн;
- **масштабируемым** — для последующих интеграций (ИЭМК, НЗ, РЭМД).