ПРОЕКТ PETITION TRUST

Персональные данные и врачебная тайна

Раздел «Проверь себя»

Проверка того, как в организации защищены персональные данные пациентов и работников: от согласий и политики до доступа в МИС, локализации баз и уведомления Роскомнадзора.

Организация: _____ **Дата проверки:** __.__.____ **Проверяющий:** _____

Как пользоваться

1. Отмечайте каждый пункт одной из трёх галочек. «Да» — требование выполнено и это можно подтвердить документом, записью или действием. «Нет» — не выполнено. «Нужна доп. проверка» — документов под рукой нет, ответ неоднозначный или подтверждение только со слов.
2. Один пункт — один проверяемый факт. Если факт не подтверждается документом или записью, ставьте «Нужна доп. проверка», а не «Да».
3. Провал — это только «Нет». «Нужна доп. проверка» провалом не считается, но такие пункты нужно закрыть в течение недели и вернуться к ним повторно.
4. Блок «Документ есть?» — входной фильтр. Если документа нет, его подпункты в основной таблице не заполняются, в колонке «Что сверить» ставится «н/д».
5. Считайте провалы только по основной таблице. Результат — не отчёт для проверяющего, а план работы: переносите провалы в раздел «Что делать дальше» с датой и ответственным.

Документ есть?

Сначала проверьте наличие документов. Если документа нет — в основной таблице его пункты не заполняются, в колонке «Что сверить» ставится «н/д».

Документ	Есть	Нет	Нужна доп. проверка	Что сверить
Д1. Политика обработки персональных данных				Опубликована, соответствует фактической обработке
Д2. Положение об обработке и защите ПДн				Роли, доступ, сроки хранения, уничтожение
Д3. Приказ об ответственном за обработку ПДн				Должность, ФИО, полномочия
Д4. Согласия пациентов и работников				Форма, цель, срок, отзыв, подпись
Д5. Модель угроз и оценка вреда субъектам				Дата, перечень угроз, меры
Д6. Журналы доступа, учёта носителей и уничтожения				Кто, когда, что, подпись

Проверка по пунктам

Ставьте любую отметку в колонке «Да», «Нет» или «Нужна доп. проверка». Пустая клетка — пункт не проверялся.

№	Что смотрим	Да	Нет	Нужна доп. проверка	НПА / что сверить
1. Документы и ответственный					
1.1	Политика обработки ПДн утверждена и доступна пациентам (найти на сайте и на стойке в холле).				152-ФЗ, ст. 18.1
1.2	Положение об обработке ПДн описывает реальные процессы: какие данные, где, кто имеет доступ (сверить с МИС).				152-ФЗ, ст. 18.1
1.3	Назначен ответственный за организацию обработки ПДн приказом (должность, ФИО, не «администратор»).				152-ФЗ, ст. 18.1

№	Что смотрим	Да	Нет	Нужна доп. проверка	НПА / что сверить
1.4	Ответственный знает свои обязанности и может их назвать (спросить, что он делает при обращении субъекта).				152-ФЗ, ст. 18.1
1.5	Перечень лиц, допущенных к обработке ПДн, утверждён и совпадает с фактическим доступом (сверить список и учётки).				152-ФЗ, ст. 19
1.6	Уведомление в Роскомнадзор об обработке ПДн подано и актуально (проверить запись в реестре операторов).				152-ФЗ, ст. 22
2. Согласия					
2.1	Согласие на обработку ПДн берётся до начала обработки, а не задним числом (сверить дату согласия и дату приёма).				152-ФЗ, ст. 3
2.2	В согласии указаны цель, перечень данных, срок и порядок отзыва (прочитать форму).				152-ФЗ, ст. 3
2.3	Отдельное согласие есть на распространение данных, если оно требуется (проверить форму).				152-ФЗ, ст. 10
2.4	Согласие на обработку сведений, составляющих врачебную тайну, оформлено отдельно, где это нужно.				323-ФЗ, ст. 13
2.5	Согласия хранятся так, что их можно найти по конкретному пациенту за 5 минут (попросить найти одно).				152-ФЗ, ст. 18
2.6	Есть процедура отзыва согласия и пример её исполнения (найти запись об отзыве).				152-ФЗ, ст. 3
2.7	Формы согласий пересмотрены после изменения процессов (посмотреть дату версии формы).				152-ФЗ, ст. 18.1
3. Модель угроз и оценка вреда					
3.1	Модель угроз безопасности ПДн разработана и утверждена (найти документ с датой).				152-ФЗ, ст. 19
3.2	Оценка вреда субъектам ПДн проведена и оформлена документом (проверить наличие и дату).				152-ФЗ, ст. 19
3.3	В модели угроз учтены реальные системы: МИС, лабораторная система, сайт, почта (сверить перечень).				152-ФЗ, ст. 19
3.4	Меры защиты из модели угроз фактически внедрены: пароли, разграничение прав, резервные копии (проверить 3 меры).				152-ФЗ, ст. 19
3.5	Модель угроз пересматривалась при изменении ИТ-инфраструктуры (посмотреть дату).				152-ФЗ, ст. 19
3.6	Ответственный за ИТ-безопасность или подрядчик назначен и отвечает за защиту (найти договор или приказ).				152-ФЗ, ст. 19
4. Доступ к МИС и журналирование					
4.1	У каждого сотрудника своя учётная запись, общие логины не используются (спросить, как входят в МИС).				152-ФЗ, ст. 19

№	Что смотрим	Да	Нет	Нужна доп. проверка	НПА / что сверить
4.2	Права доступа соответствуют должности: регистратор не видит заключения, врач не видит лишнего (проверить 3 учётки).				152-ФЗ, ст. 19
4.3	Доступ уволенных сотрудников закрывается в день увольнения (сверить 3 записи об увольнении и учётки).				152-ФЗ, ст. 19
4.4	Журналирование доступа к ПДн включено и логи хранятся (попросить показать журнал за неделю).				152-ФЗ, ст. 19
4.5	Журналы просматриваются: есть записи о выявленных нарушениях доступа (спросить, кто смотрит логи).				152-ФЗ, ст. 19
4.6	Выгрузка данных на личные устройства и флешки запрещена и технически ограничена (проверить).				152-ФЗ, ст. 19
4.7	Доступ к медкартам и результатам анализов выдаётся пациенту по документу, удостоверяющему личность.				323-ФЗ, ст. 13
5. Локализация баз и передача данных					
5.1	Базы ПДн граждан РФ размещены на серверах на территории России (запросить у ИТ сведения о размещении).				152-ФЗ, ст. 18
5.2	Требование локализации выполняется с 01.07.2025: проверены все системы, включая облачные (сверить перечень).				23-ФЗ от 28.02.2025, ч. 5 ст. 18
5.3	Передача данных в ЕГИСЗ идёт по защищённым каналам и в установленном объёме (сверить договор и настройки).				323-ФЗ, ст. 13
5.4	Передача ПДн третьим лицам (лаборатории, страховые, подрядчики) оформлена договором и согласием.				152-ФЗ, ст. 3
5.5	Список получателей ПДн известен и ограничен, «на всякий случай» данные не передаются.				152-ФЗ, ст. 19
5.6	Трансграничная передача, если есть, заявлена и разрешена (проверить, нет ли иностранных сервисов).				152-ФЗ, ст. 19
6. Уничтожение носителей и подрядчики					
6.1	Уничтожение ПДн по истечении срока хранения выполняется и оформляется актом (найти 2 акта).				152-ФЗ, ст. 19
6.2	Носители уничтожаются так, что восстановление невозможно: бумага измельчается, диски стираются (спросить, как).				152-ФЗ, ст. 19
6.3	Учёт носителей ПДн ведётся: выдача, возврат, уничтожение (проверить журнал).				152-ФЗ, ст. 19
6.4	Подрядчики, имеющие доступ к ПДн (клининг, ИТ, архив), связаны договором с условием о конфиденциальности.				152-ФЗ, ст. 19
6.5	Доступ подрядчиков ограничен и журналируется (спросить, как контролируют ИТ-подрядчика).				152-ФЗ, ст. 19

№	Что смотрим	Да	Нет	Нужна доп. проверка	НПА / что сверить
6.6	Помещения с носителями ПДн запираются, документы не лежат на столах в открытом виде (пройти).				152-ФЗ, ст. 19
7. Обращения субъектов и инциденты					
7.1	Есть порядок приёма обращений субъектов ПДн и ответственный за ответ (найти документ).				152-ФЗ, ст. 18
7.2	Срок ответа на обращение соблюдается — 10 рабочих дней с возможным продлением (сверить 3 обращения).				152-ФЗ, ст. 18
7.3	Есть журнал обращений с датами поступления и ответа (проверить заполнение).				152-ФЗ, ст. 18
7.4	Инциденты утечки фиксируются и разбираются, есть план реагирования (спросить, что делают при утечке).				152-ФЗ, ст. 19
7.5	Уведомление Роскомнадзора об инциденте направляется в установленный срок (найти порядок и шаблон).				152-ФЗ, ст. 19
7.6	Персонал знает, кому сообщать об утечке или потере носителя (спросить 3 сотрудников).				152-ФЗ, ст. 18.1
7.7	За нарушения предусмотрена ответственность, и персонал об этом информирован (проверить запись обучения).				ст. 13.11 КоАП

Итог

Критичных провалов: _____

0–2 — порядок. Документы есть, они работают и подтверждаются записями. Держите режим пересмотра.

3–5 — риск. Отдельные провалы есть, но система держится. Закройте их в течение 30 дней.

6 — на границе, считай по самому тяжёлому пункту. Если среди провалов есть пункт из блока ИСМП, персонала или лицензии — считайте, что провалов больше.

7–10 — необходим пересмотр. Работа по документам не выстроена: требуются решения сверху, а не точечные правки на местах.

Больше 10 — начинайте с разделов, где провалов больше всего, и повторите проверку через 90 дней, а не через год.

Что делать дальше

1. Соберите в одну папку политику, положение, приказ об ответственном, модель угроз и оценку вреда — это первый запрос любого инспектора.
2. Проверьте три учётные записи в МИС: права должны соответствовать должности, уволенные — закрыты.
3. Возьмите пять согласий и сверьте дату подписи с датой первого приёма: согласие не должно быть позже.
4. Запросите у ИТ сведения о размещении баз и передаче данных в ЕГИСЗ — с 01.07.2025 локализация обязательна.
5. Проверьте журнал обращений субъектов ПДн и сроки ответов, назначьте ответственного за инциденты.

Дисклеймер

Чек-лист — инструмент самопроверки. Он не заменяет проверку надзорного органа и не является юридическим заключением. Нормативная база указана по состоянию на ноябрь 2026 года; редакции нормативных актов и локальных документов следует сверять на дату проверки.