



МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ ИРКУТСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«УСТЬ-ОРДЫНСКИЙ ПРОТИВОТУБЕРКУЛЕЗНЫЙ ДИСПАНСЕР»

П Р И К А З

04.05.2017

№ 23

п. Усть-Ордынский

**«Об утверждении перечня
документов, направленных
на обеспечение выполнения
обязанностей, предусмотренных
Федеральным Законом
«О персональных данных»**

В соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами оператора», постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и руководствуясь Уставом,

ПРИКАЗЫВАЮ:

1. Назначить ответственного за организацию обработки персональных данных в ОГБУЗ Усть-Ордынский противотуберкулезный диспансер с целью структурированного подхода к организации обработки персональных данных в соответствии с требованиями законодательства - инженера энергетика В.А. Гыргеева.
2. Утвердить документы, определяющие политику в отношении обработки персональных данных:

2.1. Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (Приложение № 1);

2.2. Правила рассмотрения запросов субъектов персональных данных или их представителей (Приложение № 2);

2.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора (Приложение № 3);

2.4. Правила работы с обезличенными данными (приложение № 4);

2.5. Перечень должностей сотрудников ответственных за проведение мероприятий по обезличиванию персональных данных (Приложение № 5);

2.6. Перечни персональных данных, обрабатываемых в информационных системах персональных данных «ЕГИСЗ» и «1С-Облако» (Приложение № 6);

2.7. Должностной регламент ответственного за организацию обработки персональных данных (Приложение № 7);

2.8. Порядок доступа сотрудников учреждения в помещения, в которых ведется обработка персональных данных (Приложение № 8);

3. Довести настоящий приказ до сведения всех сотрудников и работников, ответственных за обработку и непосредственно осуществляющих обработку персональных данных под роспись;

4. Настоящий приказ опубликовать для обнародования на официальном сайте в информационно-телекоммуникационной сети общего пользования;

5. Контроль за исполнением настоящего приказа оставляю за собой;

6. Настоящий приказ вступает в силу со дня его официального опубликования на официальном сайте.

Главный врач



Д.С. Александрова

Правила

обработки персональных данных, устанавливающих процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющих для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.
3. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки и не должны быть избыточными по отношению к заявленным целям их обработки.
7. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
8. Меры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством:
 - 8.1. осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных согласно Федерального закона от 27.07.2006г. № 152-ФЗ "О персональных данных" (далее - Федеральный закон) и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
 - 8.2. оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

8.3. ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

9. Обеспечение безопасности персональных данных достигается, в частности:

9.1. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

9.2. применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

9.3. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

9.4. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

9.5. учетом машинных носителей персональных данных;

9.6. обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

9.7. восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

9.8. установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

10. Целями обработки персональных данных работников являются:

10.1. обеспечение соблюдения законов и иных нормативных правовых актов;

10.2. соблюдение порядка и правил приема на государственную гражданскую службу;

10.3. использование в уставной деятельности с применением средств автоматизации или без таких средств, включая хранение этих данных в архивах и размещение в информационно-телекоммуникационных сетях с целью предоставления доступа к ним;

10.4. заполнение базы данных автоматизированной информационной системы в целях повышения эффективности и быстрого поиска, проведения мониторинговых исследований, формирования статистических и аналитических отчетов в вышестоящие органы;

10.5. обеспечение личной безопасности работников.

11. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

12. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение

неправомерной обработки персональных данных лицом, действующим по поручению оператора.

13. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

14. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

15. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 (тридцати) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

16. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных.

17. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

18. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

Правила рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, за исключением случаев, установленных частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (с последующими изменениями) (далее - Федерального закона), в том числе содержащей:
 - 1.1. подтверждение факта обработки персональных данных оператором;
 - 1.2. правовые основания и цели обработки персональных данных;
 - 1.3. цели и применяемые оператором способы обработки персональных данных;
 - 1.4. наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
 - 1.5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
 - 1.6. сроки обработки персональных данных, в том числе сроки их хранения;
 - 1.7. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
 - 1.8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;
 - 1.9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
 - 1.10. иные сведения, предусмотренные Федеральным законом или другими федеральными законами.
2. При получении запроса субъекта персональных данных или его представителя Управление транспорта и связи города Пензы обязано сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.
3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. Запросы субъектов персональных данных или их представителей регистрируются в журнале учета запросов субъектов персональных данных или их представителей по форме, представленной в приложении к настоящим Правилам. Журнал учета запросов субъектов персональных данных или их представителей ведется ответственным за организацию обработки персональных данных.

6. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

8. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 7 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих Правил, должен содержать обоснование направления повторного запроса.

9. Оператор отказывает субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 7 и 8 настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

Приложение
к Правилам рассмотрения
запросов субъектов персональных
данных или их представителей

Журнал
учета запросов субъектов персональных данных или их представителей

N п/п	Ф.И.О. субъекта персональных данных или его представителя	Вид и реквизиты документа, удостоверяющего личность субъекта персональных данных или его представителя, реквизиты доверенности представителя субъекта персональных данных	Дата обращения	Результат исполнения запроса (ознакомление, предоставление документов (указать их реквизиты), отказ)
1	2	3	4	5

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в ОГБУЗ Усть-Ордынский противотуберкулезный диспансер (далее – диспансер), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления медицинских услуг, требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами оператора», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3. Для обработки персональных данных сотрудников и пациентов, необходимых для обеспечения деятельности в информационных системах "1С-Облако" и "ЕГИСЗ", в соответствии с Трудовым кодексом Российской Федерации,

1.4. Пользователем ИСПДн (далее – Пользователь) является сотрудник диспансера, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.5. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн диспансера проводятся в следующих целях:

- 1.5.1 проверка выполнения требований организационно-распорядительной документации по защите информации в администрации действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- 1.5.2 оценка уровня осведомленности и знаний работников администрации в области обработки и защиты персональных данных;
- 1.5.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

2.1. Проверки соответствия обработки ПДн установленным требованиям в диспансере разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (Приложение А) далее – План и предназначены для осуществления контроля выполнения требований в области защиты информации в диспансере.

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии (Приложение Б) по информационной безопасности, которая создается на период проведения данных мероприятий. Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.2.6 общий срок контрольных мероприятий не должен превышать пяти рабочих дней, при необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируются в Журнале учета событий информационной безопасности.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. отчет передается на рассмотрение руководству администрации.

4.4. Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в Протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации (Приложение В).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных администрации.

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, выполняются следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации.
- Соблюдение Порядка доступа в помещения администрации, где ведется обработка персональных данных.
- Знание Пользователями положений, инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.
- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации.
- Порядок и условия применения средств защиты информации.
- Состояние учета машинных носителей персональных данных.
- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

Приложение А
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите персональных данных

ПЛАН внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн.	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных

Контроль соблюдения режима защиты.	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения антивирусной политики.	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения парольной политики.	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена (Интернет).	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Контроль обновления ПО и единообразия применяемого ПО.	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Контроль обеспечения резервного копирования.		Ежемесячно	Ответственный за обеспечение безопасности персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности ПДн.		Ежегодно	Ответственный за обеспечение безопасности персональных данных
Поддержание в актуальном состоянии нормативно - организационные документы		Ежемесячно	Ответственный за обеспечение безопасности персональных данных

Приложение Б
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите персональных данных

Состав комиссии
осуществляющей внутреннюю проверку контроля
соответствия обработки персональных данных
в ОГБУЗ Усть-Ордынский противотуберкулезный диспансер

Председатель комиссии:

Гыргеев
Василий Александрович

- инженер-энергетик

Секретарь комиссии:

Шопконкова

- юрист-консульт

Туяна Алексеевна

Члены комиссии:

1. Михеева

- заведующий врач-методист

Вероника Борисовна

2. Барбаева

- заведующий врач-фтизиатр

Римма Петровна

3. Бадлуева

- главная медицинская сестра

Светлана Борисовна

Приложение В

к Правилам осуществления

внутреннего контроля соответствия

обработки персональных данных

требованиям к защите персональных данных

ПРОТОКОЛ № ____

**проведения внутренних проверок контроля соответствия обработки
персональных данных требованиям к защите персональных данных
в ОГБУЗ Усть-Ордынский противотуберкулезный диспансер**

наименование структурного подразделения

Настоящий Протокол составлен в том, что « ____ » _____ 20 ____ г.

(комиссией)

(должность, Ф.И.О. сотрудника)

проведена проверка _____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями:

(название документа)

В ходе проверки проверено:

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений: _____

Председатель комиссии: инженер-энергетик _____ В.А. Гыргеев

Секретарь комиссии:
юрист-консульт _____ Т.А. Шопконкова

Члены комиссии:

Заведующий врач-методист _____ В.Б. Михеева

Заведующий врач-фтизиатр _____ Р.П. Барбаева

главная медицинская сестра _____ С.Б. Бадлуева

Правила работы с обезличенными персональными данными

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами оператора» и определяют порядок работы с обезличенными данными.

2. Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

- **персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- **обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных к конкретному субъекту персональных данных, без использования дополнительной информации.

3. Условия обезличивания

3.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных.

3.2. Хранение обезличенных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, то есть обезличенные данные должны обладать свойствами, сохраняющими основные характеристики персональных данных, но не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом.

3.3. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом».

3.4. Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки.

3.2. Способы и методы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт);
- метод перемешивания (перестановка отдельных записей, а так же групп записей в массиве персональных данных).
- деление сведений на части и обработка в разных информационных системах.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. В соответствии с Перечнем должностей:

- руководитель принимает решение о необходимости обезличивания персональных данных;
- ответственный за организацию обработки персональных данных, начальники структурных подразделений готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания;
- сотрудники, осуществляющие непосредственно обработку персональных данных в связи с реализацией трудовых отношений, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание персональных данных.

4. Порядок работы с обезличенными персональными данными

4.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

4.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

4.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

4.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

**Перечень
должностей сотрудников ответственных за проведение мероприятий по
обезличиванию персональных данных**

№ п.п.	Наименование должности	Примечание
1.	Главный врач	Принимает решение о необходимости обезличивания персональных данных
2.	1. Заведующий врач-методист; 2. Заведующий врач-фтизиатр 3. Главная медицинская сестра. 4. инженер-энергетик	Готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания
3.	1. Врач-фтизиатр; 2. Врач-рентгенолог.	Непосредственно производят обезличивание персональных данных

1. ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ
обрабатываемых в информационной системе персональных данных
«ЕГИСЗ»

№ п/п	Наименование персональных данных	Срок хранения
1	фамилия	75 лет
2	имя	
3	отчество	
4	серия, номер паспорта, кем и когда выдан	
5	гражданство	
6	дата рождения	
7	место рождения	
8	адрес проживания	
9	адрес по прописке	
10	ИНН	
11	СНИЛС	
12	сведения о доходах	
13	Сведения о заработной плате	
14	Исполнительные листы	
15	Лицевые счета	
16	Место работы	
17	Сведения о квалификации	
18	Наименование образовательного учреждения	
19	Документ о подтверждении образования	
20	Ученая степень	
21	Ученое звание	
22	Беременность	
23	Временная нетрудоспособность	
24	Данные о доверенности и доверенном лице	
25	Сведения о контрагентах	

2. ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ
обрабатываемых в информационной системе персональных данных
«1С-Облако»

№ п/п	Наименование персональных данных	Срок хранения
1	фамилия	75 лет

2	имя	
3	отчество	
4	серия, номер паспорта, кем и когда выдан	
5	гражданство	
6	дата рождения	
7	место рождения	
8	адрес проживания	
9	адрес по прописке	
10	ИНН	
11	СНИЛС	
12	сведения о доходах	
13	Сведения о заработной плате	
14	Исполнительные листы	
15	Лицевые счета	
16	Место работы	
17	Сведения о квалификации	
18	Наименование образовательного учреждения	
19	Документ о подтверждении образования	
20	Ученая степень	
21	Ученое звание	
22	Беременность	
23	Временная нетрудоспособность	
24	Данные о доверенности и доверенном лице	
25	Сведения о контрагентах	

ДОЛЖНОСТНОЙ РЕГЛАМЕНТ
лица, ответственного за организацию обработки персональных данных
в ОГБУЗ Усть-Ордынский противотуберкулезный диспансер

1. Общие положения

1.1. Настоящий регламент определяет основные функции, обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных (далее – лицо, ответственное за организацию обработки персональных данных).

1.2. Лицо, ответственное за организацию обработки персональных данных назначается соответствующим распоряжением главного врача учреждения.

1.3. Лицо, ответственное за организацию обработки персональных данных руководствуется в своей деятельности законодательными актами и нормативными правовыми актами в области обработки персональных данных, а также настоящим регламентом.

1.4. Лицо, ответственное за организацию обработки персональных данных обязано знать следующие нормативные и методические документы:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации",
- Указ Президента РФ от 06.03.1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера",
- постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- Постановление Правительства Российской Федерации от 15.09.2008 г. N 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами оператора»;

- другие локальные нормативные акты и методические документы в области защиты персональных данных.

2. Должностные обязанности

Для выполнения возложенных на него функций лицо, ответственное за организацию обработки персональных данных обязано:

- ознакомить сотрудников, допущенных к обработке персональных данных, под роспись с документами, определяющими политику в отношении обработки персональных данных и иными локальными нормативными актами, необходимыми для ознакомления;

- организовать сбор с сотрудников, допущенных к обработке персональных данных, письменного обязательства о соблюдении режима конфиденциальности персональных данных субъекта и соблюдении правил их обработки;

- проводить периодические инструктажи работников по вопросам обеспечения обработки и защиты персональных данных;

- осуществлять прием субъектов персональных данных по вопросам обработки и защиты персональных данных указанных субъектов;

- по запросу субъекта персональных данных сообщать ему сведения об обработке его персональных данных, в том числе ознакомить с Правилами обработки персональных данных;

- по запросу субъекта персональных данных организовать уточнение, блокирование или уничтожение персональных данных указанного субъекта или указывать работникам, уполномоченным на требуемую операцию с персональными данными, на необходимость проведения указанной операции;

- вести журнал учета обращений субъектов персональных данных;

- осуществлять контроль за выполнением разовых или периодических мероприятий по обеспечению безопасности персональных данных;

- отслеживать изменения законодательства о персональных данных и вносить в установленном порядке корректировки к соответствующим локальным нормативным актам;

- осуществлять сопровождение и решение вопросов проверочной комиссии уполномоченного органа по защите прав субъектов персональных данных при проведении проверки;

- осуществлять контроль и учет передачи персональных данных по запросам третьих лиц/организаций.

3. Права

Для осуществления своих обязанностей лицо, ответственное за обработку персональных данных имеет следующие права:

- указывать работникам, допущенным к обработке персональных данных, на необходимость выполнения установленных мер по обеспечению безопасности персональных данных;
- не допускать работников до обработки персональных данных до подписания ими письменного обязательства о неразглашении персональных данных;
- воздействовать на лиц, ответственных за разовые или периодические мероприятия по обеспечению безопасности персональных данных, в вопросах готовности указанных мероприятий;
- право доступа ко всем носителям персональных данных;
- право доступа ко всем локальным нормативным актам в области обработки и защиты персональных данных;
- указывать лицам, участвующим в обработке персональных данных, на необходимость осуществления уточнения, блокирования или уничтожения персональных данных по запросу субъекта;
- вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящим регламентом.

4. Ответственность

Лицо, ответственное за организацию обработки персональных данных несет ответственность за:

- осведомленность работников, участвующих в обработке персональных данных, в вопросах обеспечения безопасности персональных данных;
- комплектность и содержание локальных нормативных актов в области защиты персональных данных;
- своевременность выполнения разовых и периодических мероприятий по обеспечению безопасности персональных данных;
- выполнение обязанностей перед субъектами персональных данных и органами, регулирующими взаимоотношения в области обработки персональных данных;
- неисполнение и ненадлежащее исполнение своих обязанностей, предусмотренных настоящим регламентом, в пределах, определенных действующим трудовым законодательством.

5. Заключительные положения

Должностной регламент подлежит пересмотру в случае изменения законодательства Российской Федерации о персональных данных, определяющего должностные обязанности ответственного за организацию обработки персональных данных.

ПОРЯДОК
доступа сотрудников диспансера в помещения,
в которых ведется обработка персональных данных

1. Основные положения.

1.1. Настоящий Порядок разработан в целях обеспечения безопасности персональных данных при их обработке (в том числе хранении) путем создания условий, в соответствии с Федеральным законом от 27 июля 2006 года № 152 ФЗ "О персональных данных" и Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами оператора», затрудняющих несанкционированный доступ к техническим средствам, участвующим в обработке персональных данных, и материальным носителям персональных данных.

1.1. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками диспансера.

1.2. Помещения, в которых ведется обработка персональных данных, должны отвечать определенным нормам и исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов и средств автоматизации.

1.3. В терминах настоящего Порядка под правом доступа в помещение понимается возможность посещения помещения без нарушения принятых норм и регламентов, не зависящая от воли других лиц.

1.4. Ознакомлению с настоящим Порядком подлежат все сотрудники диспансера, имеющие право доступа в помещения, в которых установлены технические средства, участвующие в обработке персональных данных, или хранятся материальные носители персональных данных (далее по тексту – помещения, в которых осуществляется обработка персональных данных), а также руководители структурных подразделений (отделов), работники которых осуществляют обработку персональных данных.

1.5. Настоящий Порядок вступает в силу с момента его утверждения и действует до его отмены либо замены новым Порядком.

2. Организация доступа в помещения, в которых осуществляется обработка персональных данных.

2.1. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

2.2. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

2.3. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники диспансера, уполномоченные на обработку персональных данных.

2.4. Нахождения лиц в помещениях диспансера, не являющихся уполномоченными лицами на обработку персональных данных, возможно только в присутствии уполномоченного на обработку персональных данных сотрудника диспансера.

2.5. Доступ в помещения, в которых осуществляется обработка персональных данных, разрешается только в рабочее время.

2.6. Доступ в помещения, в которых осуществляется обработка персональных данных, в нерабочее время возможен только по письменной заявке сотрудника, согласованной с его непосредственным руководителем и имеющей разрешающую резолюцию руководителя. Данные заявки хранятся у лица, ответственного за организацию обработки персональных данных в диспансере.

2.7. Последний работник, покидающий помещение, в котором осуществляется обработка персональных данных, обязан закрыть его на ключ, при этом запрещается оставлять ключ в замке помещения.

2.8. Лица, имеющие право доступа в помещение, в котором осуществляется обработка персональных данных, несут ответственность за недопущение пребывания в помещении сотрудников диспансера, не имеющих права доступа в данное помещение, и сторонних лиц в отсутствие лиц, имеющих право доступа в данное помещение.

2.9. В случае утраты ключей от помещений, ставится в известность ответственного за организацию обработки персональных данных и немедленно заменяется замок.

2.10. Уборка в помещениях, где ведется обработка персональных данных, производится только в присутствии сотрудников, работающих в этих помещениях.

2.11. При обнаружении повреждений запоров или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка персональных данных, эти помещения не вскрываются, а составляется акт о случившемся, и немедленно ставится в известность главного врача диспансера и органы МВД.

2.12. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с лицом, ответственным за организацию обработки персональных данных в диспансере.

3. Контроль соблюдения порядка доступа в помещения, в которых осуществляется обработка персональных данных.

3.1. Контроль за соблюдением настоящего Порядка осуществляется лицом, ответственным за организацию обработки персональных данных в диспансере.

3.2. Лицо, ответственное за организацию обработки персональных данных, в случае установления факта нарушения сотрудником диспансера настоящего Порядка проводит с данным сотрудником разъяснительную работу, а в случае неоднократного нарушения уведомляет главного врача диспансера.

Приложение А к Порядку доступа сотрудников диспансера в помещения, в которых ведется обработка персональных данных.

Перечень защищаемых помещений.

№ п/п	Наименование помещения	Адрес и место расположения
1	Кабинет №113 «Отдел кадров»	п. Усть-Ордынский, ул. Содружества, 30, 1-этаж.
2	Кабинет № 138 «Приемный покой»	п. Усть-Ордынский, ул. Содружества, 30, 1-этаж.
3	Кабинет № 148 «Амбулаторное отделение»	п. Усть-Ордынский, ул. Содружества, 30, 1-этаж.
4	Кабинет № 153 «Амбулаторное отделение»	п. Усть-Ордынский, ул. Содружества, 30, 1-этаж.
5	Кабинет № 145 «Клиника- диагностическая лаборатория»	п. Усть-Ордынский, ул. Содружества, 30, 1-этаж.
6	Кабинет № 132	п. Усть-Ордынский, ул.

	«Бактериологическая лаборатория»	Содружества, 30, 1-этаж.
7	Кабинет № 149 «Организационно-методический кабинет»	п. Усть-Ордынский, ул. Содружества, 30, 1-этаж.
8	Кабинет №117 «Бухгалтерия»	п. Усть-Ордынский, ул. Содружества, 30, 1-этаж.
9	Кабинет № 239 «Заведующая стационарным отделением»	п. Усть-Ордынский, ул. Содружества, 30, 2-этаж.
10	Кабинет № 241 «Ординаторская»	п. Усть-Ордынский, ул. Содружества, 30, 2-этаж.
11	Кабинет № 237 «Кабинет врачебной комиссии»	п. Усть-Ордынский, ул. Содружества, 30, 2-этаж.
12	Кабинет № 340 «Старшая медсестра»	п. Усть-Ордынский, ул. Содружества, 30, 3-этаж.
13	Кабинет «Ординаторская»	п. Усть-Ордынский, ул. Ербанова, 26, 1-этаж.

Приложение Б
к Порядку доступа сотрудников
диспансера в помещения, в которых
ведется обработка персональных данных.

**Лица имеющие право доступа в защищаемые помещения,
в которых ведется обработка персональных данных**

Нумерация кабинетов	Допущенные лица
Кабинет №113 (1-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Шопконкова Туяна Алексеевна 2. Бальхеева Анна Григорьевна 3. Курбатова Татьяна Анатольевна
Кабинет № 138 (1-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Жигжитова Баирма Борисовна 2. Шелковникова Людмила Владимировна
Кабинет № 148 (1-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Мотошкина Вера Архиповна 2. Бартуева Марина Александровна
Кабинет № 153 (1-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Бартуева Марина Александровна 2. Васильева Инга Борисовна
Кабинет № 145 (1-этаж) (п. Усть-Ордынский,	Алсаева Людмила Сергеевна

ул. Содружества, 30)	
Кабинет № 132 (1-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	Харимаева Елена Ильинична
Кабинет № 149 (1-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Михеева Вероника Борисовна 2. Хахалова Нэлли Прокопьевна
Кабинет № 117 (1-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Мясникова Ирина Николаевна 2. Алсаева Татьяна Анатольевна
Кабинет № 239 (2-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	Барбаева Римма Петровна
Кабинет № 241 (2-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Алсаева Елена Романовна 2. Бартуева Марина Александровна 3. Асалханова Татьяна Александровна
Кабинет № 237 (2-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Еланов Юрий Андреевич 2. Филиппова Татьяна Павловна 3. Барбаева Римма Петровна 4. Бартуева Марина Александровна 5. Алсаева Елена Романовна 5. Хамукова Лия Леонидовна 6. Мотошкина Вера Архиповна 7. Асалханова Татьяна Александровна 8. Аржитова Елена Викторовна 9. Бальхеева Екатерина Николаевна 10. Николаева Лариса Николаевна 11. Номогоева Александра Константиновна 12. Наталинова Тамара Владимировна
Кабинет № 340 (3-этаж) (п. Усть-Ордынский, ул. Содружества, 30)	1. Миронова Лидия Николаева 2. Боксоева Ирина Ивановна 3. Бадмаева Ольга Васильвна 4. Бадлуева Светлана Борисовна
Кабинет «Ординаторская» (п. Усть-Ордынский, ул. Ербанова, 26)	1. Хамукова Лия Леонидовна 2. Мотошкина Вера Архиповна 3. Бадмаева Лада Васильевна 4. Манжеева Виктория Борисовна 5. Боксоева Ирина Ивановна