1.Цели и основные задачи СПб ГБУЗ МИАЦ

2. Цели и задачи Положения

2.1. Область применения

2.2. Определения и термины, упомянутые в Положении и приложениях

3. Обязанности и ответственность сотрудников в сфере информационной политики

3.1. Обязанности и ответственность руководителей организации

3.2. Обязанности и ответственность работников организации

3.3. Обязанности и ответственность привлекаемых для работы с информацией сторонних лиц и организаций

3.4. Юридическая ответственность работников СПб ГБУЗ МИАЦ за несоблюдение Положения

4. Управление информационными ресурсами

4.1. Сбор данных

4.2. Регистрация и документирование информации

4.3. Обработка и хранение данных

4.4. Систематизация данных

4.5. Анализ данных

4.6. Категории хранения

4.7. Правила защиты и хранения данных

4.8. Продолжительность хранения данных

4.9. Хранение и архивирование информации

4.10. Обновление и поддержание актуальности информации

4.11. Порядок и контроль доступа и обеспечение безопасности данных

4.12. Отчетность и контроль за исполнением Положения при работе с информацией

5. Раскрытие и предоставление информации

5.1. Условия и порядок раскрытия информации при взаимодействии с третьими лицами

5.2. Правила предоставления информации государственным органам

5.3. Правила предоставления информации контролирующим организациям

5.4. Правила предоставления информации иным лицам

6. Использование и развитие ресурсов для управления информацией

6.1. Эффективное использование информационных ресурсов

6.2. Развитие инфраструктуры

6.3. Обучение и подготовка персонала

6.4. Мониторинг и анализ

6.5. Инновации и технологическое обновление

6.6. Сотрудничество с внешними партнерами

7. Контроль исполнения

7.1. Механизмы контроля за выполнением информационной Положения

7.2. Аудит и проверка информационных систем

7.2.1. Технический аудит

7.2.2. Проверка информационных ресурсов

7.2.3. Ревизия процедур доступа

7.2.4. Аудит безопасности

7.2.5. Документация и отчетность

8. Мероприятия при обнаружении нарушений в сфере сохранности информации

8.1. Определение видов нарушений

8.2. Проведение расследования по факту информационных инцидентов и нарушений

8.3. Документирование нарушений в сфере сохранности информации

8.4. Процедура обжалования

8.5. Корректирующие действия в организации при обнаружении нарушений в сфере сохранности информации

8.5.1. Устранение последствий

8.5.2. Обучение и повышение квалификации

9. Обновление и пересмотр Положения

9.1. Основания для обновления

9.2. Аудит и процедура обновления Положения организации

9.3. Документирование и внедрение

10. Заключение.

**Введение**

Настоящая Положение об информационной политики Санкт-Петербургского государственного бюджетного учреждения здравоохранения "Медицинский информационно-аналитический центр (далее — СПб ГБУЗ МИАЦ)", (далее - Положение) разработана в соответствии с требованиями законодательства Российской Федерации в сфере здравоохранения и информационной безопасности. Положение направлена на обеспечение конфиденциальности, доступности и актуальности медицинской информации, а также на повышение качества медицинской помощи и достижение целей и задач СПб ГБУЗ МИАЦ.

* 1. **Цели и основные задачи СПб ГБУЗ МИАЦ**

**Цели:**

**Повышение качества медицинской помощи**:

Создание условий для улучшения качества и доступности медицинской помощи через формирование единого информационного пространства в сфере здравоохранения.

**Интеграция информационных систем:**

Участие в создании и эксплуатации единой государственной информационной системы в сфере здравоохранения для эффективного обмена данными между медицинскими организациями.

**Обеспечение управленческих решений:**

Организационно-методическое обеспечение доступа к данным и ресурсам для поддержки управленческих решений в области здравоохранения.

Развитие цифровых технологий: Реализация политики цифровой трансформации, включая внедрение новых технологий и обеспечение безопасности информационных систем.

**Анализ и улучшение:**

Постоянный мониторинг данных, анализ больших данных и внедрение инновационных технологий для достижения целей и задач в области здравоохранения.

**Основные задачи:**

Формирование единого информационного пространства:

Создание и развитие инфраструктуры для интеграции медицинских данных на территории субъекта Российской Федерации.

**Поддержка федеральных проектов:**

Участие в реализации федерального проекта по созданию единого цифрового контура в здравоохранении.

**Методическое обеспечение:**

Организационно-методическое сопровождение внедрения и эксплуатации информационных систем и технологий в медицинских организациях.

**Доступ к данным:**

Обеспечение доступа к необходимой информации для принятия управленческих решений и мониторинга эффективности системы здравоохранения.

**Внедрение новых технологий:**

Участие в проектировании и разработке программного обеспечения для автоматизации процессов в медицинских учреждениях.

**Обучение и поддержка:**

Проведение обучающих мероприятий и техническая поддержка пользователей информационных систем.

**Анализ данных:**

Сбор, обработка, хранение и анализ данных в сфере здравоохранения, включая медицинскую статистику и демографическую информацию.

**Сотрудничество и координация:**

Организация взаимодействия между медицинскими организациями, государственными органами и другими участниками системы здравоохранения.

**Обеспечение безопасности:**

Разработка и внедрение мер по защите информации и обеспечению безопасности значимых объектов критической информационной инфраструктуры.

* 1. **Цели и задачи Положения**

**Цель:** Создание условий для эффективного использования информационных ресурсов и технологий в интересах достижения целей и задач СПб ГБУЗ МИАЦ.

**Задачи:**

а) **Законность и защищенность**: Обработка и хранение данных осуществляется строго в соответствии с законодательством Российской Федерации, регулирующим сбор, хранение, обработку, защиту и уничтожение как конфиденциальной, так и другой информации, включая медицинскую. Данная задача описана в Положении о политике информационной безопасности СПб ГБУЗ МИАЦ.

б) **Доступность:**

Обеспечение доступа к информации для уполномоченных сотрудников и посетителей в рамках их полномочий и с соблюдением требований законности. Используются современные технологии для автоматизации процессов сбора, обработки и анализа данных, что позволяет своевременно получать необходимую информацию.

в) **Интегрированность**:

Объединение информационных систем и ресурсов в единую информационную систему, что улучшает взаимодействие между различными подразделениями и организациями здравоохранения для повышения качества обслуживания пациентов в медучреждениях города и посетителей, а также для достижения других целей СПб ГБУЗ МИАЦ.

г) **Актуальность:**

Обеспечение своевременного обновления и актуализации данных для принятия обоснованных управленческих решений. Постоянный мониторинг и анализ информации позволяют выявлять и устранять проблемные области, способствуя достижению целей СПб ГБУЗ МИАЦ.

д) **Обучение и развитие:**

Организация непрерывного обучения и повышения квалификации работников в области информационной безопасности. Реализация программ обучения с использованием современных образовательных технологий и методических материалов, учитывающих специфику медицинских данных и требования информационной безопасности.

е) **Внедрение политики импортозамещения:**

С акцентом на снижение зависимости от иностранных информационно-коммуникационных технологий и замену их отечественными аналогами.

ж) **Развитие информационных технологий в Организации:**

Усовершенствование бизнес-процессов в организации с помощью IT-решений направлено на более качественное решение целей и задач Организации. Внедрение передовых IT-решений для автоматизации бизнес-процессов для улучшения, ускорение и точность обработки данных для решения целей и задач Организации.

..

**2.1. Область применения**

Это положение распространяется на все виды деятельности в СПб ГБУЗ МИАЦ, связанные с использованием и защитой информационных ресурсов. Положение охватывает все процессы управления, обработки, хранения и передачи информации, включая персональные данные пациентов, внутренние документы, данные о медицинских услугах и финансовые операции. Оно применяется ко всем сотрудникам организации, включая руководителей и работников Организации, административные и вспомогательные службы, а также к третьим лицам, которым может быть предоставлен доступ к информационным системам СПб ГБУЗ МИАЦ в рамках профессиональной деятельности или выполнения контрактных обязательств.

2.2. Определения и термины, упомянутые в Положении и приложениях

В этом разделе представлены основные понятия и термины, используемые в рамках настоящего положения. Они призваны обеспечить единое понимание всех аспектов Политики в Организации см. Приложение № 1. «Определения и термины в сфере информационной политики.

**3. Обязанности и ответственность сотрудников в сфере информационной политики**

3.1. **Обязанности и ответственность руководителей Организации**

**Обязанность:** Разработка, утверждение и контроль исполнения внутренних документов (политики, положения, стратегии, инструкции). Бюджетирование и контроль за расходованием средств на проекты в сфере информационной политики. Взаимодействие с регуляторами и другими компетентными органами по вопросам применения Положения. Обеспечение ведения всех документационных процедур в соответствии с Приложением №3 "Положение о документообороте".

**Ответственность:** Обеспечение выполнения целей и задач Положения, адекватное расходование бюджета. См. п.3.4.

3.2. **Обязанности и ответственность работников Организации**

**Обязанность:** Соблюдение установленных правил и процедур в области сбора, обработки, передачи и удаления информации. Немедленное информирование руководства о любых инцидентах, связанных с утечкой, искажением или потерей данных. Регулярное прохождение обучения по повышению квалификации в сфере информационной политики с акцентом на следующие темы: защита данных, реагирование на инциденты, использование защищенных коммуникационных каналов.

**Ответственность:** См. п.3.4.

3.3. **Обязанности и ответственность привлекаемых для сбора, обработки, передачи и уничтожения информации сторонних лиц и организаций**

**Обязанность:** Соблюдение условий договоров и соглашений, касающихся обработки информации, включая соответствие стандартам безопасности данных, предусмотренным законодательством РФ. Информирование Организации о всех обнаруженных уязвимостях или инцидентах, которые могут повлиять на законность, защищенность, доступность и целостность данных.

**Ответственность:** См. п.3.4.

3.4. **Юридическая ответственность за несоблюдение Положения**

За нарушение обязанностей предусмотрены административные и уголовные санкции в соответствии с ТК РФ, КоАП РФ, УК РФ и ГК РФ. Для сторонних лиц и организаций — санкции в соответствии с ГК РФ, КоАП РФ и УК РФ. Детализация санкций представлена в Приложении №5 "Законодательные санкции в сфере Положения".

* 1. **Управление информационными ресурсами**

Управление информационными ресурсами — ключевая задача, обеспечивающая безопасное и эффективное использование данных в организации.

В этой главе рассматриваются методы и процессы, которые помогают оптимизировать сбор, обработку, хранение и анализ информации.

Особое внимание уделяется соблюдению законодательных требований и обеспечению безопасности данных на всех этапах их жизненного цикла.

**4.1 Регистрация и документирование информации**

**Регистрация**: Ведение реестров и журналов учета для отслеживания движения и изменений информации, включая даты создания, изменения, доступа и удаления.

**Документация**: Оформление всех документов, связанных с управлением информацией, включая протоколы, отчеты и служебные записки.

**4.2 Хранение и архивирование информации**

**Хранение**: Определение мест хранения информации с учетом ее категории и уровня конфиденциальности, включая физическое и электронное хранение.

**Архивирование**: Реализация процедур архивирования устаревших данных для их сохранности и облегчения доступа в будущем, в соответствии с требованиями законодательства и внутренними регламентами.

**4.3 Актуализация и обновление информации**

**Актуализация данных**: Регулярное обновление информации для поддержания ее актуальности, включая проверку, корректировку и добавление новых сведений.

**Обновление регистров**: Обновление записей в регистрах учета при изменении данных или поступлении новой информации.

**4.4 Контроль доступа и безопасность данных**

**Контроль доступа**: Установление правил и процедур доступа к информации, включая определение прав и обязанностей сотрудников Процедура доступа .

**Безопасность**: Применение мер защиты информации, включая физическую, техническую и организационную безопасность для предотвращения несанкционированного доступа. См. Положение об информационной безопасности.

**4.5 Отчетность и аудит**

**Отчетность**: Регулярное предоставление отчетов о состоянии и движении информации в соответствии с внутренними и внешними требованиями.

**Аудит**: Проведение регулярных проверок и аудитов для оценки эффективности учета информации и соблюдения процедур.

**4.6 Правила защиты и хранения данных**

Установление процедур и стандартов защиты и хранения данных, соответствующих требованиям конфиденциальности и безопасности.

**4.7 Продолжительность хранения данных**

Определение сроков хранения различных категорий данных с учетом законодательных и операционных требований.

**4.8 Хранение и архивирование**

Управление процессами хранения и архивирования информации для обеспечения ее сохранности и доступности.

**4.9 Обновление и поддержание актуальности информации**

Регулярное обновление и пересмотр информации для поддержания ее релевантности и точности.

**4.10 Порядок и контроль доступа и обеспечение безопасности**

Разработка и внедрение механизмов контроля доступа для обеспечения безопасности и защиты информационных активов.

**4.11 Отчетность и контроль за исполнением Положения при работе с информацией**

Организация системы отчетности и мониторинга для контроля за соблюдением положений и правил работы с информацией.

1. . **Раскрытие и предоставление информации**

**5.1. Условия и порядок раскрытия информации при взаимодействии с третьими лицами**

Определяет сценарии, при которых информация может быть раскрыта третьим лицам в соответствии с законодательными требованиями, договорными обязательствами или управленческими потребностями. Все запросы должны быть оформлены письменно и проверены на соответствие законодательству и внутренней политике конфиденциальности.

5**.2. Правила предоставления информации государственным органам**

Регламентирует процесс предоставления информации государственным органам, включая официальные запросы и сопровождающие документы. Обеспечивает протоколирование всех действий, связанных с предоставлением данных, и соблюдение законодательных требований.

5.3**. Правила предоставления информации контролирующим организациям**

Описывает процедуры предоставления информации при проведении аудитов и проверок, устанавливает требования к документации и отчетности, и гарантирует соблюдение норм и условий, определенных контрактами и законодательством.

**5.4. Правила предоставления информации иным лицам**

Устанавливает механизмы предоставления информации не связанным напрямую с государственными или контролирующими организациями лицам, включая необходимость учета согласия субъектов данных и ограничение доступа по требованиям конфиденциальности и данных, согласованных с запрашивающими сторонами.

**6. Использование и развитие ресурсов для управления информацией**

**6.1. Эффективное использование информационных ресурсов**

Эффективное использование информационных ресурсов включает в себя максимизацию их потенциала для достижения целей организации. Это означает оптимизацию процессов сбора, хранения, обработки и распространения информации для повышения продуктивности и сокращения издержек.

**6.2. Развитие инфраструктуры**

Развитие инфраструктуры направлено на модернизацию и расширение технических средств и программного обеспечения. Включает в себя обновление серверов, сетевых устройств и систем хранения данных для обеспечения высокой доступности и надежности информационных систем.

**6.3. Обучение и подготовка персонала**

Обучение и повышение квалификации персонала направлены на развитие навыков работы с новыми технологиями и информационными системами. Регулярные тренинги и семинары помогают сотрудникам оставаться в курсе последних тенденций в области информационной безопасности и управления данными.

**6.4. Мониторинг и анализ**

Мониторинг и анализ информационных систем позволяют отслеживать и оценивать их эффективность. Использование аналитических инструментов и метрик для оценки производительности систем и определения областей для улучшения.

**6.5. Инновации и технологическое обновление**

Внедрение новых технологий и постоянное технологическое обновление улучшают процессы управления информацией. Использование искусственного интеллекта, машинного обучения и облачных решений для автоматизации и повышения точности работы с данными.

**6.6. Сотрудничество с внешними партнерами**

Сотрудничество с внешними партнерами и поставщиками технологических решений расширяет возможности организации в области управления информацией. Партнерства могут включать совместные исследования, разработку программного обеспечения и обмен опытом для улучшения информационных процессов.

**7. Контроль исполнения**

**7.1. Механизмы контроля за выполнением информационной политики**

Назначение ответственных: Определение и назначение сотрудников, ответственных за непосредственный контроль выполнения информационной политики.

Разработка процедур: Установление четких процедур и регламентов для обеспечения соблюдения политики по обработке и защите данных.

Мониторинг и отчетность: Регулярное мониторинг соблюдения информационной политики и предоставление отчетов о выполнении установленных требований.

**7.2. Аудит и проверка информационных систем**

**7.2.1. Технический аудит:** Оценка технической инфраструктуры и систем безопасности на соответствие стандартам и требованиям информационной безопасности.

**7.2.2. Проверка информационных ресурсов:** Анализ состояния информационных ресурсов, включая их соответствие политикам конфиденциальности и управления данными.

**7.2.3. Ревизия процедур доступа:** Проверка наличия и эффективности процедур контроля доступа к информационным системам и данным.

**7.2.4. Аудит безопасности:** Осуществление комплексного аудита мер безопасности, включая анализ угроз и уязвимостей, а также тестирование на проникновение.

7.2.5. Документация и отчетность: Создание и поддержание актуализированной документации по всем процессам и процедурам, связанным с информационной безопасностью, и предоставление отчетности руководству о результатах аудитов и проверок.

**8. Мероприятия при обнаружении нарушений в сфере сохранности информации**

**8.1. Определение видов нарушений**

Классификация нарушений: Разработка и применение классификационной системы для определения различных типов информационных нарушений, включая утечки данных, несанкционированный доступ и нарушение процедур безопасности.

**8.2. Проведение расследования по факту информационных инцидентов и нарушений**

Расследование инцидентов: Немедленное проведение расследований при обнаружении нарушений для установления обстоятельств и причин происшествий.

**8.3. Документирование нарушений в сфере сохранности информации**

Ведение документации: Создание подробных отчетов о каждом нарушении, включая данные о времени, месте, участниках и последствиях нарушения.

**8.4. Процедура обжалования**

Обжалование решений: Разработка процедуры, позволяющей сотрудникам и другим заинтересованным сторонам обжаловать решения, связанные с обработкой информационных инцидентов и нарушений.

**8.5. Корректирующие действия в организации при обнаружении нарушений в сфере сохранности информации**

**8.5.1. Устранение последствий**: Проведение мероприятий по минимизации ущерба от нарушений, включая восстановление данных и усиление мер безопасности.

**8.5.2. Обучение и повышение квалификации:** Организация целевых обучающих программ для сотрудников по повышению осведомленности и компетенций в области информационной безопасности.

**9. Обновление и пересмотр Положения**

**9.1. Основания для обновления**

Изменения в законодательстве: Адаптация Положения к новым законам и нормативным актам, касающимся обработки и защиты информации.

Технологические изменения: Интеграция новых технологий, требующих пересмотра процессов управления данными и обеспечения безопасности.

Обратная связь и рекомендации: Внесение изменений на основе обратной связи от сотрудников и результатов внутренних аудитов.

**9.2. Аудит и процедура обновления** Положения организации

Планирование аудита: Организация регулярных аудитов для оценки актуальности и эффективности действующего Положения.

Процесс аудита: Проведение аудита с участием внутренних и/или внешних аудиторов для глубокого анализа всех аспектов положения и выявления потребностей в его изменении.

Анализ результатов: Обработка результатов аудита и формирование предложений по обновлению Положения.

**9.3. Документирование и внедрение**

Документация изменений: Формирование документов, отражающих все изменения и обновления в Положении.

Процедуры утверждения: Организация процесса утверждения изменений руководством и введение их в действие.

Внедрение обновлений: Распространение обновленного Положения среди сотрудников и организация обучающих сессий и семинаров для ознакомления с новыми процедурами и стандартами.

1**0. Заключение**

В заключении данного документа подчеркивается важность постоянного мониторинга и адаптации информационной политики организации для соответствия текущим законодательным требованиям и технологическим изменениям. Это обеспечивает не только защиту конфиденциальности и целостности информации, но и поддерживает высокий уровень доверия среди клиентов и партнеров.

Реализация установленных процедур и норм, описанных в Положении, требует совместных усилий всех сотрудников и управленческих структур. Регулярное обучение, пересмотр процедур, и адаптация к новым условиям являются ключевыми элементами в поддержании актуальности и эффективности информационной безопасности организации.

Организация должна оставаться бдительной и реагировать на любые вызовы, связанные с защитой данных, чтобы сохранить свою репутацию и обеспечить соблюдение прав и интересов всех заинтересованных сторон.