УТВЕРЖДАЮ

Главный врач МБУ «ЦГБ №2 А.А. Мислявского»

_____ К.Н. Савинов

«_____» _____ 2016 г.

М.П.

Политика в области обработки и защиты персональных данных в МБУ «ЦГБ №2 А.А. Мислявского»

г. Екатеринбург

2016 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика в области обработки и защиты персональных данных (далее – Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и действует в отношении всей информации, которую Муниципальное бюджетное учреждение «Центральная городская больница № 2 им. А.А. Мислявского» (далее – МБУ «ЦГБ №2 А.А. Мислявского»), может получить в рамках осуществления своей деятельности. Политика разработана в соответствии Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и предназначена для ознакомления неограниченного круга лиц.

В Политике определены требования к персоналу оператора, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных (ИСПДн) оператора.

Целью настоящей Политики является обеспечение безопасности объектов защиты оператора информационной системы от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для субъектов ПДн.

Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Требования настоящей Политики распространяются на всех работников МБУ «ЦГБ №2 А.А. Мислявского» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (пациенты, родители, законные представители, подрядчики, аудиторы и т.п.).

2. ПРАВОВОЙ РЕЖИМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Субъекты персональных данных

В МБУ «ЦГБ №2 А.А. Мислявского» обрабатываются персональные данные следующих категорий физических лиц (субъектов персональных данных):

- работников (лиц, состоящих в трудовых отношениях с МБУ «ЦГБ №2 А.А. Мислявского»);
- работников (по гражданско-правовым договорам);

- пациентов МБУ «ЦГБ №2 А.А. Мислaвского», а также их родителей и законных представителей;
- иных лиц, давших согласие на обработку своих персональных данных, либо сделавших общедоступными свои персональные данные или чьи персональные данные получены из общедоступного источника, а также в других случаях, предусмотренных законодательством Российской Федерации.

2.2. Категории обрабатываемых персональных данных

МБУ «ЦГБ №2 А.А. Мислaвского» обрабатывает следующие категории персональных данных:

а) Работники: фамилия, имя, отчество; данные паспорта (серия, номер, кем и когда выдан); дата и место рождения; адрес места жительства и регистрации; индивидуальный номер налогоплательщика (ИНН); номер страхового свидетельства (СНИЛС); контактный телефон; сведения о доходах; информация об образовании и повышении квалификации; сведения о составе семьи; сведения о социальных льготах; данные военного билета, отношения к воинской обязанности; данные о состоянии здоровья, данные о трудовой деятельности и стаже (место работы, должность, период работы, дата приема, увольнения); личная фотография; личная характеристика; другие данные в том числе вносимые в личную карточку работника (форма Т-2).

б) Пациенты: фамилия, имя, отчество; данные паспорта (серия, номер, кем и когда выдан); данные свидетельства о рождении; данные медицинского полиса; контактная информация (телефон, e-mail), адрес прописки, адрес проживания; социальный статус; категория льготы; место работы/учебы; профессия; состояние здоровья (анамнез жизни и заболевания, данные результатов обследования, информация о привитости, диагноз, лечение).

в) Родители пациентов, законные представители: фамилия, имя, отчество; данные паспорта (серия, номер, кем и когда выдан); контактная информация (телефон, e-mail), адрес прописки, адрес проживания.

2.3. Цели обработки персональных данных

МБУ «ЦГБ №2 А.А. Мислaвского» осуществляет обработку персональных данных в следующих целях:

а) Работников: содействие в трудовой деятельности, обеспечение личной безопасности, учет результатов исполнения договорных обязательств, осуществление безналичных платежей на счет работника, обеспечение работоспособности и сохранности ресурсов и имущества работодателя, осуществление коллективного взаимодействия и совместного использования информационных ресурсов, аттестация, повышение квалификации, а также наиболее полное

исполнение обязательств и компетенций в соответствии с Трудовым кодексом Российской Федерации, и другими нормативно-правовыми актами в сфере трудовых отношений.

б) Пациентов, родителей, законных представителей: с целью исполнения требований законодательства РФ (Федерального закона от 21.11.2011г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» и др.), а также договорных отношений.

в) Субъектов персональных данных (подрядчиков, аудиторов и т.п): с целью исполнения договорных отношений.

2.4. Правовое основание обработки персональных данных

МБУ «ЦГБ №2 А.А. Мислявского» осуществляет обработку персональных данных на основании:

- Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ;
- Гражданского кодекса Российской Федерации от 18.12.2006 г. № 230-ФЗ;
- Федерального закона от 07.07.2003 г. № 126-ФЗ «О связи»;
- Федерального закона от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федерального закона от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федерального закона от 28.03.1998 г. № 53-ФЗ «О воинской обязанности и военной службе»;
- Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Устава МБУ «ЦГБ №2 А.А. Мислявского».

2.5. Перечень действий с персональными данными

МБУ «ЦГБ №2 А.А. Мислявского» осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных с использованием средств автоматизации, а также без использования таких средств.

МБУ «ЦГБ №2 А.А. Мислaвского» может поручить обработку персональных данных третьим лицам в случаях, если:

- на оператора персональных данных возложены законодательством Российской Федерации функций, полномочия и обязанности;
- субъект дал согласие на осуществление таких действий (при наличии условий в договоре с третьим лицом о соблюдении им принципов и правил обработки персональных данных, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»);
- в других случаях, предусмотренных законодательством Российской Федерации.

Трансграничная передача персональных данных не осуществляется.

2.6. Права субъекта

Субъект персональных данных, согласно законодательству Российской Федерации, имеет право:

- получать информацию, касающуюся обработки своих персональных данных;
- требовать уточнения своих 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;
- требовать прекращение обработки своих персональных данных в случаях, предусмотренных законодательством Российской Федерации;
- обжаловать действия или бездействие МБУ «ЦГБ №2 А.А. Мислaвского» в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

2.7. Оценка вреда, меры по обеспечению безопасности персональных данных

Таблица 1. Соотношение возможного вреда и принимаемых мер

№ п/п	Категории данных	Оценка вреда	Меры по обеспечению безопасности
1.	Общедоступные персональные данные; Первичные учетные данные (ФИО, пол)	**не приводит** к негативным последствиям для субъектов персональных данных	назначение лица, ответственного за организацию обработки персональных данных
2.	Контактная информация (место жительства, место	**может привести** к незначительным негативным	назначение лица, ответственного за организацию обработки персональных данных; издание

№ п/п	Категории данных	Оценка вреда	Меры по обеспечению безопасности
	работы, дата и место рождения, номер телефона и т.п.)	последствиям для субъектов персональных данных	локальных актов по вопросам обработки персональных данных; определение перечня обрабатываемых персональных данных и защищаемых информационных ресурсов, мест хранения; учет лиц, получивших доступ к персональным данным, и лиц, которым такая информация была передана или предоставлена; ознакомление работников, обрабатывающих персональные данные, с локальными актами и законодательством Российской Федерации в области обработки персональных данных; принятие организационных и технические мер по защите персональных данных, закрепление в инструкциях и положениях; осуществление внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных».
3.	Сведения о реквизитах (данные паспорта, индивидуальный номер налогоплательщика, номер страхового свидетельства - СНИЛС); социальное положение (гражданство; сведения о составе семьи; сведения о воинском учете; сведения о социальных льготах; знание иностранных языков и т.п.); трудовая деятельность (доход, информация об образовании и повышении квалификации)	**может привести** к негативным последствиям для субъектов персональных данных	назначение лица, ответственного за организацию обработки персональных данных; издание локальных актов по вопросам обработки персональных данных; определение перечня обрабатываемых персональных данных и защищаемых информационных ресурсов, мест хранения; установление правил и ограничение доступа к персональным данным; учет лиц, получивших доступ к персональным данным; ознакомление работников, обрабатывающих персональные данные, с локальными актами и законодательством Российской Федерации в области обработки персональных данных; принятие организационных и технических мер по защите персональных данных, которые закреплены в инструкциях и положениях; осуществление внутреннего контроля и аудита соответствия обработки персональных данных Федеральному

№ п/п	Категории данных	Оценка вреда	Меры по обеспечению безопасности
			закону от 27.07.2006 № 152-ФЗ «О персональных данных».

2.8. Условия прекращения обработки персональных данных

Срок или условие прекращения обработки персональных данных в МБУ «ЦГБ №2 А.А. Мислaвского»:

- ликвидация МБУ «ЦГБ №2 А.А. Мислaвского» или прекращение деятельности;
- по истечению 75 лет - хранение персональных данных работников;
- по исполнению обязательств по договорам и в течение срока исковой давности;
- отзыв согласия, если иное не предусмотрено Федеральным законодательством, либо в течение срока хранения документов согласно установленным срокам хранения для определенных категорий документов, если иное не предусмотрено Федеральным законодательством.

2.9. Меры, применяемые для защиты персональных данных

МБУ «ЦГБ №2 А.А. Мислaвского» принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных граждан - субъектов персональных данных.

К таким мерам относятся:

- назначение ответственного лица за организацию обработки персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;
- разработка документов, определяющие политику МБУ «ЦГБ №2 А.А. Мислaвского» в отношении обработки персональных данных, локальных документов по вопросам обработки персональных данных;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, с требованиями к защите персональных данных, с документами, определяющими политику МБУ «ЦГБ №2 А.А. Мислaвского» в отношении обработки персональных данных, локальными документами по вопросам обработки персональных данных;
- опубликование в сети Интернет документа, определяющего политику МБУ «ЦГБ №2 А.А. Мислaвского» в отношении обработки персональных данных;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение прошедшей в установленном порядке процедуры оценки соответствия средств защиты информации;
- систематическое осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;
- осуществление контроля над выполнением принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.9.1. Методы защиты персональных данных

Методами защиты персональных данных являются:

- реализация разрешительной системы допуска к обработке персональных данных;
- ограничение доступа в помещения, где размещены технические средства, осуществляющие обработку персональных данных, а также хранятся носители информации;
- разграничение доступа к персональным данным;
- регистрация действий сотрудников, контроль несанкционированного доступа к персональным данным;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи.

3. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сотрудники оператора, являющиеся пользователями информационных система персональных данных (ИСПДн), должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники оператора, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.

При работе с ПДн в ИСПДн сотрудники оператора обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов.

При завершении работы с ИСПДн сотрудники обязаны защитить монитор с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники оператора должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили данную политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

3.1. Должностные обязанности сотрудников, обрабатывающих персональные данные.

Должностные обязанности сотрудников, обрабатывающих персональные данные описаны в следующих документах:

- Положении, регламентирующем порядок и условия обработки персональных данных работников МБУ «ЦГБ №2 А.А. Мислaвского»;

- Должностные инструкции лиц, непосредственно осуществляющего обработку ПД (Ответственность лица, непосредственно осуществляющего обработку ПД);
- Инструкция при возникновении внештатных ситуаций (по действиям в случае компрометации ключевой информации).

3.2. Ответственность сотрудников оператора

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного Кодекса Российской Федерации).

Сотрудники оператора несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками оператора правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников оператора.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

МБУ «ЦГБ №2 А.А. Мислaвского» имеет право вносить изменения в настоящую Политику. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее утверждения и размещения в общедоступном месте, если иное не предусмотрено новой редакцией Политики.