Приложение №3
к приказу №-3-П
от 09.01.2025 г.
ГБУЗ РБ Стоматологическая
поликлиника №2 г.Уфа

«УТВЕРЖДАЮ»
Главный врач
ГБУЗ РБ Стоматологическая
поликлиника №2 г. Уфа
_____ О.Б. Визгалова
«09» января 2025 г.

Положение об обработке персональных данных

УФА-2025

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по обеспечению защиты сведений конфиденциального характера (далее - Положение) регламентирует единый порядок обращения с документами в ГБУЗ РБ СП №2 г. Уфа (далее - Учреждение), содержащими сведения ограниченного доступа.

1.2. Настоящее Положение не распространяется на порядок работы со сведениями, относящимися к государственной тайне.

1.3. Конфиденциальная информация не подлежит разглашению кроме случаев, предусмотренных действующим законодательством РФ и настоящим Положением.

1.4. Ответственность за организацию и обеспечение сохранности конфиденциальной информации и выполнение мероприятий по ее защите возлагается на главного врача Учреждения, его обособленных и внутренних структурных подразделений.

1.5. Меры по обеспечению защиты сведений конфиденциального характера включают в себя:

- определение перечня конфиденциальной информации;
- ограничение доступа к конфиденциальной информации, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- регулирование отношений по использованию конфиденциальной информации на основании трудовых и гражданско-правовых договоров.

1.6. Меры по обеспечению защиты сведений, составляющих врачебную тайну, дополнительно включают в себя:

- учёт лиц, получивших доступ к информации, составляющей врачебную тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- нанесение на материальные носители, содержащие информацию, составляющую врачебную тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Конфиденциально» с указанием обладателя такой информации.

1.7. Настоящая политика может быть пересмотрена в связи изменениями законодательства Российской Федерации в области обеспечения информационной безопасности.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Врачебная тайна - сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (ч.1 ст. 13 Закона № 323-ФЗ).

Гриф секретности – реквизит, свидетельствующий о степени секретности сведений, содержащихся в их носителе, проставляемый на самом носителе секретной информации и (или) указываемый в сопроводительной документации на него.

Документ - информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать.

Информация - сведения (сообщения, данные) независимо от формы их представления (Федеральный закон №149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»).

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (Федеральный закон №149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»).

Обладатель информации - лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (Федеральный закон №149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»).

Ответственный за делопроизводство – сотрудник Учреждения, на которого возложены обязанности по организации и ведению делопроизводства в Учреждении.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон №152-ФЗ от 27 июля 2006 г. «О персональных данных»).

Подразделение информационной безопасности – Отдел информационной безопасности Учреждения.

Разглашение конфиденциальной информации - действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации, либо вопреки трудовому или гражданско-правовому договору.

3. КЛАССИФИКАЦИЯ ИНФОРМАЦИИ

Политикой информационной безопасности Учреждения установлена следующая классификация информации:

Общедоступная - информация публикуемая, хранящаяся в свободных источниках (справочники, печатные издания, интернет), определена для свободного распространения.

Ограниченного доступа - не может иметь свободного распространения, и/или быть раскрытой, опубликованной, в связи с интересами обладателя информации и требованиями законодательства/контрагентов по обеспечению конфиденциальности. Информация ограниченного доступа по критерию доступности делится на внутреннюю и конфиденциальную.

Внутренняя - информация без ограничения внутреннего доступа, предназначенная для совместной работы внутри Учреждения и может быть доступна всем сотрудникам, но не может быть распространена/предоставлена сторонним лицам. Примеры внутренней информации: внутренний справочник телефонов без ограничительных отметок, информационные письма и т.п.

Конфиденциальная - информация с ограничением внутреннего и внешнего доступа. Доступ предоставляется только в соответствии с принципом служебной необходимости по решению обладателя информации. Доступ может предоставляться как к конкретному документу, так и к группе документов, объединенных признаком. К конфиденциальной информации безоговорочно относится информация, содержащая персональные данные, врачебную тайну, а также любую другую информацию, отнесенную обладателем информации к конфиденциальной.

4. РАЗРАБОТКА ПЕРЕЧНЯ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

4.1. Для подготовки Перечня сведений конфиденциального характера (далее – Перечень) и поддержания его в актуальном состоянии, приказом по Учреждению создается постоянно действующая Экспертная комиссия.

4.2. Перечень разрабатывается Экспертной комиссией на основе предложений руководителей структурных подразделений и утверждается главным врачем Учреждения. При

подготовке предложений о внесении сведений в Перечень, руководителями структурных подразделений должны быть учтены вероятные экономические и иные последствия, включая ущерб, который может быть нанесен интересам Учреждения, интересам иных лиц, вследствие бесконтрольного распространения информации.

4.3. Если информацию невозможно классифицировать в соответствии со сведениями, содержащимися в действующем Перечне, но она, по мнению исполнителя, может быть использована в ущерб интересам Учреждения и иных лиц, исполнитель должен представить в подразделение информационной безопасности аргументированные предложения о необходимости защиты этой информации и внесении изменений (дополнений) в Перечень. До принятия окончательного решения, защита этой информации должна быть обеспечена как если бы она была указана в Перечне.

4.4. Утвержденный Перечень доводится до сведения:

- структурных подразделений Учреждения - в полном объеме;
- контрагентов Учреждения - в объеме, определяемом договором (контрактом, соглашением).

4.5. Перечень пересматривается не реже, чем раз в год с целью внесения изменений и дополнений. Основаниями для снятия ранее введенных ограничений на распространение информации являются:

- изменение действующего Перечня, на основании которого ограничения были введены;
- получение письменного разрешения обладателя информации на ее раскрытие.

4.6. Решение о снятии ранее введенных ограничений на распространение информации принимается Экспертной комиссией и утверждается главным врачем Учреждения:

- по предложениям руководителей структурных подразделений, в ведении которых находятся документы, содержащие конфиденциальную информацию;
- по предложениям подразделения информационной безопасности;
- по результатам проведения Экспертной комиссией проверки документов.

5. ПОРЯДОК РЕГИСТРАЦИИ ВХОДЯЩЕЙ И ИСХОДЯЩЕЙ КОРРЕСПОНДЕНЦИИ УЧРЕЖДЕНИЯ, СОДЕРЖАЩЕЙ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

5.1. Регистрация входящей и исходящей корреспонденции, содержащей информацию конфиденциального характера, должна осуществляться Управлением делами в справочниках «Входящие РКК»/«Исходящие РКК» системы электронного документооборота Учреждения и/или журналах на бумажном носителе (далее - Журналы) только после проверки соответствия перечня конфиденциальных документов сопроводительному письму или описи к документам. В случае отсутствия во входящей корреспонденции одного или нескольких документов, указанных в сопроводительном листе или описи, Ответственный за делопроизводство оформляет в установленном порядке в двух экземплярах Акт приема-передачи в котором указывает фактически полученные документы, один экземпляр отправляет отправителю документов, второй прикрепляет к полученным документам.

5.2. Регистрации в Журналах подлежат все входящие/исходящие сведения конфиденциального характера вне зависимости от того, получены ли они по почте, переданы нарочно или созданы в Учреждении.

5.3. Документы, содержащиеся во входящей корреспонденции, могут иметь проставленные обладателем информации гриф ограничения доступа: «Для служебного пользования», «Конфиденциально» или грифы отнесения информации к категориям, охраняемым согласно законодательству РФ. Гриф «Для служебного пользования», как правило, используют органы государственной власти.

5.4. Хранение входящей корреспонденции ограниченного доступа, копий исходящих документов конфиденциального характера, а также документов, с грифом «Для служебного пользования», «Конфиденциально», осуществляется в запираемом шкафу.

5.5. При передаче документов конфиденциального характера главному врачу и его заместителям, конверты к конфиденциальным документам хранятся у Ответственного за

делопроизводство запираемом шкафу. Конверты не вскрываются, так как могут содержать информацию, предназначенную только для исполнителей.

5.6. Направление конфиденциальных документов для ознакомления может осуществляться на бумажном носителе или через систему электронного документооборота с помощью соответствующего типового маршрута. При этом осуществляется шифрование документов на открытых ключах получателей и проставление электронной подписи на документе. При отсутствии сертификатов электронной подписи, сотрудники обращаются в подразделение информационной безопасности. Если исполнитель просрочил срок по задаче, Ответственный за делопроизводство выясняет причину и принимает меры для ознакомления должностного лица с документом.

5.7. При направлении исходящей корреспонденции исполнитель обязан проверить, не относятся ли сведения к конфиденциальным, сверив с Перечнем сведений конфиденциального характера. В случае возникновения оснований отнесения предоставляемой информации к категории конфиденциальной и отсутствия указанной информации в перечне сведений конфиденциального характера необходимо сообщить об этом в подразделение информационной безопасности. Подразделение информационной безопасности инициирует внесение изменений Экспертной комиссией в Перечень.

5.8. Гриф «Для служебного пользования» на документы на бумажных носителях, содержащих конфиденциальную информацию, проставляются в правом верхнем углу первой страницы документа.

5.8.1. Если конфиденциальные документы имеют сопроводительное письмо, не содержащее конфиденциальную информацию, то на сопроводительном письме проставляется гриф с пометкой «при наличии приложения», и гриф проставляется на первом листе каждого документа, приложенного к сопроводительному письму, содержащего конфиденциальную информацию.

5.8.2. Если документы на бумажных носителях, содержащие конфиденциальную информацию, имеют приложения, *указанные в тексте документа*, то гриф проставляется только в правом верхнем углу первой страницы документа, на приложения гриф не проставляется.

5.8.3. Если приложения к документу *не указаны в тексте документа*, то гриф проставляется на самом документе и на каждом приложении.

5.9. Документы, содержащие конфиденциальную информацию, в общем случае, могут располагаться на следующих видах материальных носителей:

- бумажные носители.
- электронные носители (Floppy/CD/DVD/HD диски, Flash-накопители и прочие).

На электронных носителях могут одновременно располагаться документы, содержащие как конфиденциальную, так и внутреннюю и/или общедоступную информацию. Если на электронном носителе расположен хотя бы один конфиденциальный документ, в отношении этого электронного носителя должны соблюдаться требования, предъявляемые к конфиденциальным документам. При невозможности проставления грифа на носитель информации, гриф проставляется в сопроводительной документации к данному носителю или к носителю прикрепляется ярлык, содержащий маркировку, позволяющую идентифицировать носитель информации.

6. ПОРЯДОК ОБРАЩЕНИЯ С ДОКУМЕНТАМИ НА МАТЕРИАЛЬНЫХ НОСИТЕЛЯХ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

6.1. Ведение делопроизводства, оформление, учет и движение документов, содержащих конфиденциальную информацию, должны осуществляться в порядке, установленном действующими законодательными, нормативными актами, настоящим Положением, а также внутренними положениями Учреждения, устанавливающими общие принципы работы с документами.

6.2. Документы, содержащие конфиденциальную информацию, должны храниться в служебных помещениях в надежно запираемых шкафах.

6.3. Предотвращение хищений носителей конфиденциальной (защищаемой) информации обеспечивается организационными и техническими мерами. К техническим мерам относятся системы контроля и управления доступом, видеонаблюдения. Организационные меры включают в себя следующие пункты:

- по окончанию рабочего дня, а также вне времени работы, носители с защищаемой информацией должны храниться в запираемых шкафах или сейфах, доступ к которым имеет уполномоченный сотрудник;
- электронные носители с защищаемой информацией запрещается оставлять без присмотра на рабочем месте;
- запрещается снимать несанкционированные копии с носителей с защищаемой информацией;
- запрещается выносить носители с защищаемой (конфиденциальной) информацией за пределы Учреждения, за исключением случаев, предусмотренных внутренними документами Учреждения.

6.4. Подразделение ИБ должно контролировать ведение, учет хранящихся в Учрежденияи конфиденциальных документов. Ведение Журналов осуществляется Ответственным за делопроизводство, назначенным приказом по Учреждения.

6.5. При смене лица ответственного за делопроизводство конфиденциальных документов согласно приказу по Учреждению, должна проводиться полная проверка путем сверки с учетными данными в Журналах. Результаты проверки должны отражаться в Акте приема-передачи конфиденциальных документов (по форме согласно приложению 1 к настоящему Положению). Акт должен утверждаться главным врачем.

6.6. Не реже, чем раз в год, с целью обеспечения сохранности конфиденциальных документов и с целью изъятия из обращения документов, потерявших актуальность, должна проводиться инвентаризация конфиденциальных документов. Проверка должна проводиться путем сверки с учетными данными в Журналах. Результаты проверки должны отражаться в Акте проверки наличия конфиденциальных документов (по форме согласно приложению 2 к настоящему Положению). Акт должен утверждаться главным врачем. Конфиденциальные документы, утратившие актуальность, должны сдаваться в архив Учреждения.

6.7. Документы, содержащие конфиденциальную информацию, направляемые третьим лицам, должны сдаваться Ответственному за делопроизводство для учета (регистрации) и рассылки с указанием списка рассылки. Не разосланные по каким-либо причинам документы, их копии, должны быть уничтожены.

6.8. Отправка третьим лицам исходящей корреспонденции на бумажных и электронных носителях, содержащей конфиденциальную информацию, осуществляется только Ответственного за делопроизводство и только заказными отправлениями или курьерами/нарочными Учреждения или получателя.

6.9. Отправка конфиденциальной информации контрагентам и клиентам с использованием электронной почты допускается при условии принятия мер по защите передаваемой информации от несанкционированного доступа. Для защиты информации от несанкционированного доступа может быть использовано шифрование информации. Подразделением ответственным за консультирование сотрудников по защите передаваемой конфиденциальной информации от несанкционированного доступа является подразделение информационной безопасности.

6.10. При отправке конфиденциальной информации с использованием электронной почты, необходимо принимать во внимание возможность возникновения конфликта интересов адресатов, поскольку адреса рассылки доступны всем получателям. Предпочтительным является отправка конфиденциальной информации с использованием электронной почты отдельно каждому получателю.

7. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

7.1. Доступ сотрудникам Учреждения (исполнителям) к конфиденциальной информации может быть предоставлен только к той информации, которая необходима им для выполнения

своих прямых должностных обязанностей. Порядок предоставления доступа устанавливается настоящим Положением и внутренним регламентом предоставления доступа к информационным ресурсам Учреждения.

7.2. Доступ сотрудникам Учреждения и третьим лицам к сведениям, содержащим персональные данные сотрудников Учреждения, предоставляется в порядке, установленном настоящим Положением и положениями об обработке и защите персональных данных в Учреждении.

7.3. Лица, привлекаемые к работе в Учреждении по трудовым соглашениям, в том числе стажеры, допускаются к работе с документами, содержащими конфиденциальную информацию в соответствии с правилами, установленными настоящим Положением.

7.4. Предоставление конфиденциальной информации по запросу органов государственной власти, органов местного самоуправления, судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, осуществляется на основании письменных мотивированных требований, которые должны быть подписаны уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации и срока предоставления этой информации, если иное не установлено федеральными законами.

7.5. Конфиденциальная информация сторонним организациям может быть представлена только по решению главного врача или главного бухгалтера.

7.6. Для предоставления доступа к конфиденциальной информации сотрудникам сторонних организаций с целью заключения или в рамках заключенных с ними договоров, с организацией должно быть подписано соглашение о неразглашении и защите конфиденциальной информации. Данное требование не распространяется на органы государственной власти, органы местного самоуправления.

7.7. Передача документов, содержащих конфиденциальную информацию сторонним организациям, производится согласно Описи документов. Один экземпляр Описи с подписью получателя передается на хранение в Ответственному за делопроизводство.

7.8. При направлении информации конфиденциального характера необходимо требовать соблюдения конфиденциальности указанной информации.

8. ПЕРЕЧЕНЬ МЕР, НАПРАВЛЕННЫХ НА ПРЕДОТВРАЩЕНИЕ НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ КОНФИДЕЦИАЛЬНОЙ ИНФОРМАЦИИ

8.1. Лица, поступающие на работу в Учреждении, должны быть ознакомлены под роспись с Перечнем сведений, относящихся к конфиденциальной информации, предупреждены об ответственности за разглашение (утрату) конфиденциальной информации.

8.2. С лицами, поступающими на работу в Учреждении, должен проводиться инструктаж о мерах по обеспечению конфиденциальности информации.

8.3. Лица, поступающие на работу в Учреждении, должны дать письменное обязательство о неразглашении конфиденциальной информации. Обязательство о неразглашении конфиденциальной информации должно храниться в личном деле сотрудника.

8.4. В трудовые договоры, заключенные с сотрудниками Учреждения, и должностные инструкции, должны быть включены положения об ответственности за разглашение (утрату) сотрудниками сведений, содержащих конфиденциальную информацию.

9. ОБЯЗАННОСТИ СОТРУДНИКОВ, ДОПУЩЕННЫХ К РАБОТЕ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

9.1. Сотрудники структурных подразделений Учреждения обязаны:

- знать и выполнять требования настоящего Положения;
- знать Перечень в части их касающейся и правильно определять категорию конфиденциальности документов;
- знакомиться только с теми документами и выполнять только те работы, к которым они допущены;

• хранить в тайне известную им конфиденциальную информацию, информировать непосредственного руководителя и сотрудников подразделения информационной безопасности об утрате документов, содержащих конфиденциальную информацию, фактах нарушения порядка обращения с ними, попытках несанкционированного доступа к ним;

• строго соблюдать порядок обращения с документами, содержащими конфиденциальную информацию, обеспечивать в процессе работы защищенность этой информации от посторонних лиц;

• при ведении деловых переговоров с представителями сторонних организаций или с частыми лицами, ограничиться выдачей минимальной информации, действительно необходимой для их успешного завершения.

• не допускать рассылки документов, содержащих конфиденциальную информацию, адресатам, к которым они не имеют отношения;

• при увольнении, сдавать полученные оригиналы конфиденциальных документов уполномоченному лицу, у которого были получены документы.

9.2. Сотрудникам Учреждения запрещается:

• разглашать или использовать конфиденциальную информацию в личных или иных целях без соответствующего разрешения;

• передавать или разглашать конфиденциальную информацию в открытой переписке, статьях или выступлениях;

• снимать копии с документов, в отношении которых установлен режим конфиденциальности, производить выписки из них или использовать различные технические средства (фото-, видео- и звукозаписывающую аппаратуру) для записи конфиденциальной информации без согласования с вышестоящим руководителем и подразделением информационной безопасности;

• выполнять на дому работы с документами, содержащими конфиденциальную информацию, а также выносить за пределы зданий документы, содержащие конфиденциальную информацию, без согласования с вышестоящим руководителем и подразделением информационной безопасности.

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ (УТРАТУ) КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И НАРУШЕНИЕ ПОРЯДКА ОБРАЩЕНИЯ С НЕЙ

10.1. Разглашение (утрата) конфиденциальной информации является инцидентом информационной безопасности и влечет за собой последствия, предусмотренные действующим законодательством РФ.

10.2. В случае выявления факта разглашения (утраты) конфиденциальной информации, подразделением информационной безопасности проводится служебное расследование согласно внутренним регламентам расследования инцидентов информационной безопасности. Сотрудник Учреждения подозреваемый в допущении разглашения (утраты) конфиденциальной информации на время проведения служебного расследования может быть отстранен от выполнения служебных обязанностей, связанных с обработкой документов, содержащих конфиденциальную информацию.

10.3. Ответственность за разглашение конфиденциальной информации несет сотрудник имевший доступ к такой информации и допустивший их разглашение (утрату) или нарушивший порядок обращения с ними.

10.4. При наличии в действиях сотрудника разгласившего (утратившего) конфиденциальную информацию признаков административного правонарушения или уголовного преступления, руководство Учреждения имеет право обратиться в правоохранительные органы для привлечения виновного к ответственности в соответствии с действующим законодательством.

10.5. При выявлении нарушений правил обращения с конфиденциальной информацией, к сотруднику Учреждения, допустившему нарушения, не приведшие к разглашению конфиденциальной информации, могут быть применены меры дисциплинарного взыскания.

10.6. Привлечение к ответственности за разглашение конфиденциальной информации третьих лиц осуществляется в порядке, определенном действующим законодательством РФ.

11. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ КОНТРОЛЯ ПОРЯДКА ОБРАЩЕНИЯ С ДОКУМЕНТАМИ, СОДЕРЖАЩИМИ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

11.1. Контроль порядка обращения с документами, содержащими конфиденциальную информацию, осуществляется в целях оценки фактического состояния защиты информации, выявления недостатков и нарушений в порядке работы с документами, установления причин таких недостатков и нарушений, выработки предложений, направленных на их устранение и предотвращение.

11.2. Целевые и текущие проверки соблюдения правил обращения с конфиденциальной информацией проводятся подразделениями информационной безопасности. Результаты проверок оформляются в виде Акта проверки и передаются на утверждение главному врачу.

11.3. Проверки проводятся в объеме требований нормативных документов, регламентирующих организацию и ведение делопроизводства документов, содержащих конфиденциальную информацию, а также порядок обращения с ними.

Приложение 1
к Положению по обеспечению защиты
сведений конфиденциального характера в
ГБУЗ РБ СП №2 г. Уфа

.

АКТ
приема-передачи конфиденциальных документов

г..... «___» _____ 202_г

Согласно приказу № ___ от ___.___.202_г. _____(фио, должность)____ передал(а), а _____(фио, должность)_____ принял(а) следующие конфиденциальные документы, зарегистрированные в журнале регистрации входящих и исходящих документов ГБУЗ РБ СП №2 г. Уфа.

В результате передачи-приема установлено:

№ п/п	Регистрационный номер документа по Журналу	Дата регистрации	Наименование документа	Наличие на момент передачи	
				По журналу	фактически
1					
2					
3					

В связи с выявлением отсутствия документов ограниченного доступа со следующими регистрационными номерами: _____

Документы согласно Акту передал_____
подпись, Ф.И. О.

Документы согласно Акту принял _____
подпись, Ф.И. О.

Приложение 2
к Положению по обеспечению защиты
сведений конфиденциального характера в
ГБУЗ РБ СП №2 г. Уфа

АКТ
проверки наличия конфиденциальных документов

г.…… «___» _____ 202_г

Мы, комиссия в составе:

Председатель
Член комиссии
Член комиссии

Согласно приказу № ___ от ___.___.202_г , проверила фактическое наличие конфиденциальных документов зарегистрированных в Журнале регистрации входящих и документов ГБУЗ РБ СП №2 г. Уфа и в Журнале регистрации исходящих документов ГБУЗ РБ СП №2 г. Уфа.

В результате инвентаризации установлено:

№ п/п	Регистрационный номер документа по Журналу	Дата регистрации	Наименование документа	Наличие на момент проверки		Решение комиссии	
				По Журналу	фактически	Сдать в архив	Уничтожить

По факту отсутствия документов ограниченного доступа со следующими регистрационными номерами:_____.

Копия настоящего Акта передана в отдел информационной безопасности для проведения служебного расследования.

Председатель комиссии: _____
Члены комиссии: _____
_____
_____

Приложение 3
к Положению по обеспечению защиты
сведений конфиденциального характера в
ГБУЗ РБ СП №2 г. Уфа

СОГЛАШЕНИЕ №
о неразглашении и защите конфиденциальной информации

«____» _____ 202_ г.

ГБУЗ РБ СП №2 г. Уфа в лице главного врача _____ _____, действующего на основании Устава с одной стороны, и _____, в лице _____, действующего на основании _____ с другой стороны, в тексте настоящего Соглашения вместе именуемые «Стороны», а в зависимости от действия с Конфиденциальной информацией Передающая Сторона или Получающая Сторона, заключили настоящее Соглашение о нижеследующем:

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Документ - информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать.

Информация - сведения (сообщения, данные) независимо от формы их представления (Федеральный закон №149-ФЗ от 27 июля 2006 г. "Об информации, информационных технологиях и о защите информации).

Конфиденциальная информация - информация, доступ к которой ограничен в соответствии с действующим законодательством Российской Федерации и настоящим Соглашением.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (Федеральный закон №149-ФЗ от 27 июля 2006 г. "Об информации, информационных технологиях и о защите информации").

Доступ к конфиденциальной информации - санкционированный процесс ознакомления с конфиденциальной информацией физического лица с согласия обладателя конфиденциальной информации или на ином законном основании, при условии сохранения конфиденциальности этой информации.

Обладатель информации - лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (Федеральный закон №149-ФЗ от 27 июля 2006 г. "Об информации, информационных технологиях и о защите информации).

Передача конфиденциальной информации - передача Передающей стороной Получающей стороне информации, являющейся конфиденциальной, по электронным каналам передачи данных или зафиксированной на материальном носителе, на основании, в объеме и на условиях, предусмотренных настоящим Соглашением, включая условие о принятии установленных Соглашением мер по охране ее конфиденциальности.

Разглашение конфиденциальной информации - действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации, либо вопреки трудовому или гражданско-правовому договору.

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. В соответствии с условиями настоящего Соглашения, Получающей стороне предоставляется доступ к Конфиденциальной информации Передающей стороны.

2.2. Конфиденциальная информация передается в целях выполнения договора от _____ №_____ и не может быть использована Получающей стороной в иных целях.

2.3. При передаче Конфиденциальной информации, Передающая сторона подтверждает и гарантирует, что:

- она является законным обладателем всей Конфиденциальной информации, передаваемой ею в соответствии с настоящим Соглашением;
- вся Конфиденциальная информация получена законным образом, и Передающая сторона имеет все права на передачу такой Конфиденциальной информации Получающей стороне;
- передаваемая Конфиденциальная информация не составляет государственную тайну Российской Федерации, и ее передача не является нарушением действующего законодательства Российской Федерации.

2.4. Каждая из Сторон обязуется обеспечить защиту Конфиденциальной информации и не допускать разглашение полученной Конфиденциальной информации в порядке, предусмотренном настоящим Соглашением.

2.5. Отношения между Сторонами по охране конфиденциальности информации регулируются действующим законодательством Российской Федерации и настоящим Соглашением.

3. ОБЯЗАННОСТИ СТОРОН

3.1. Получающая сторона обязуется:

3.1.1. Соблюдать в отношении Конфиденциальной информации, полученной от Передающей стороны, такой же режим конфиденциальности, как и в отношении своей собственной Конфиденциальной информации.

3.1.2. Самостоятельно определять способы защиты Конфиденциальной информации, полученной по Соглашению, кроме способов, которые Сторона обязана применять в соответствии с настоящим Соглашением.

3.1.3. Не разглашать Конфиденциальную информацию, а также в одностороннем порядке не прекращать действие режима конфиденциальности.

3.1.4. Без письменного согласия Передающей стороны не использовать Конфиденциальную информацию в личных целях и не передавать ее третьим лицам, как в период действия договора, так и в течение трех лет после прекращения настоящего Соглашения.

3.1.5. При получении Конфиденциальной информации или доступа к ней, подписать Акт приёма-передачи конфиденциальной информации (Приложение 1 к Соглашению).

3.1.6. Передать Передающей стороне список сотрудников Получающей стороны, допущенных к полученной Конфиденциальной информации, оформленный на фирменном бланке Получающей стороны, подписанный руководителем и заверенный печатью Получающей стороны (Приложение 2 к Соглашению). В случае дополнения (изменения) списка, Передающей стороне представляется новый список

3.1.7. Информировать Передающую сторону об изменении контактных лиц, в соответствии с п. 8.1. Соглашения.

3.1.8. Обеспечить, чтобы третьи лица, допускаемые к Конфиденциальной информации по согласованию с Передающей стороной, до получения доступа к Конфиденциальной информации приняли на себя письменные обязательства по неразглашению Конфиденциальной информации в объеме не меньшем, чем установлено в Соглашении.

3.1.9. Незамедлительно сообщить Передающей стороне о допущенном Получающей стороной, либо ставшем ей известном факте разглашения, незаконном получении или незаконном использовании Конфиденциальной информации третьими лицами.

3.1.10. Не раскрывать факт существования настоящего Соглашения, кроме случаев, предусмотренных п. 3.2.2. настоящего Соглашения, либо с письменного согласия Передающей стороны.

3.1.11. Немедленно уведомить в письменной форме Передающую сторону о поступлении запроса или требовании о предоставлении или передаче Конфиденциальной информации

Передающей стороны от уполномоченных государственных органов, их должностных лиц, направленного в случае и порядке, предусмотренных Федеральными законами Российской Федерации, с указанием объема и характера передаваемой информации.

3.1.12. При проведении расследования фактов разглашения Конфиденциальной информации, включить в состав комиссии по расследованию данных инцидентов представителей Передающей стороны.

3.1.13. Обеспечить доступ специалистов Передающей стороны, в случае указанном в п. 3.1.12. Соглашения, к оценке условий хранения переданной Конфиденциальной информации и принимаемых мер по обеспечению режима конфиденциальности.

3.1.14. После получения письменного требования Передающей стороны, а также при прекращении, расторжении Соглашения и в случае реорганизации или ликвидации Получающей стороны, возвратить в течение десяти календарных дней, за свой счет, по Акту приема-передачи Конфиденциальной информации (Приложение 1 к Соглашению) Передающей стороне все полученные оригиналы и копии носителей Конфиденциальной информации или уничтожить по Акту все оригиналы и копии Конфиденциальной информации, включая размноженные экземпляры, в любой форме, находящиеся в распоряжении Получающей стороны, а также в распоряжении лиц, которым конфиденциальная информация была передана в соответствии с п. 3.1.8. настоящего Соглашения. Один экземпляр Акта об уничтожении предоставить Передающей стороне.

3.2. Получающая сторона вправе:

3.2.1. Предоставлять Конфиденциальную информацию своим должностным лицам (работникам), а также агентам, советникам и иным лицам, связанным с Получающей стороной гражданско-правовыми договорами, которым, по обоснованной оценке Получающей стороны, необходимо знать эту Конфиденциальную информацию в связи с осуществлением взаимодействия Сторон, и которые связаны с Получающей стороной обязательствами о неразглашении Конфиденциальной информации.

3.2.2. Предоставлять Конфиденциальную информацию только по мотивированному требованию уполномоченных государственных органов, их должностных лиц, организаций только в случаях и порядке, предусмотренных действующим законодательством Российской Федерации.

3.2.3. Использовать опыт и знания, полученные в процессе исполнения обязательств по настоящему Соглашению, в своей деятельности, не связанной с данным взаимодействием.

3.3. Передающая сторона обязуется:

3.3.1. При передаче Конфиденциальной информации или доступа к ней, оформить и подписать Акт приёма-передачи конфиденциальной информации (Приложение 1 к Соглашению).

3.3.2. Конфиденциальную информацию, представляемую на материальном носителе (в письменном или электронном виде) в соответствии с настоящим Соглашением, передавать с явным обозначением конфиденциальности.

3.3.3. Извещать в письменной форме Получающую сторону об изменении и отмене режима конфиденциальности в отношении переданной Конфиденциальной информации.

3.3.4. Информировать Получающую сторону об изменении контактных лиц, в соответствии с п. 8.1. Соглашения.

3.3.5. Предоставить Получающей стороне заверенный список сотрудников Передающей стороны, уполномоченных для взаимодействия с Получающей стороной по вопросам Конфиденциальной информации.

3.4. Передающая сторона вправе:

3.4.1. Устанавливать, изменять и отменять в письменной форме режим конфиденциальности в отношении переданной Конфиденциальной информации.

3.4.2. Разрешать или запрещать доступ к Конфиденциальной информации, согласовывать порядок и условия доступа к Конфиденциальной информации третьих лиц, согласно п. 3.1.8. Соглашения.

3.4.3. Требовать от юридических и физических лиц, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена

Конфиденциальная информация или получивших доступ к Конфиденциальной информации, соблюдения режима конфиденциальности этой информации.

3.4.4. Требовать от лиц, получивших доступ к Конфиденциальной информации в результате действий, осуществленных случайно или по ошибке, соблюдения режима конфиденциальности этой информации.

3.4.5. Защищать в установленном действующим законодательством Российской Федерации порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами Конфиденциальной информации, в том числе требовать возмещения убытков, причиненных в связи с нарушением прав Передающей стороны.

3.4.6. Направлять, по согласованию с Получающей стороной, специалистов для работы в составе комиссии согласно п. 3.1.12. Соглашения.

3.4.7. Направить Получающей стороне письменное требование о возврате или уничтожении всех оригиналов и копий Конфиденциальной информации или любой ее части.

4. ИСКЛЮЧЕНИЕ

4.1. Настоящим Стороны подтверждают, что Конфиденциальная информация не получает защиту в соответствии с настоящим Соглашением, и Получающая сторона не ограничивается в ее использовании, разглашении и распространении в случаях:

4.1.1. Если Конфиденциальная информация в течение действия настоящего Соглашения или до истечения указанного в п. 7.1. настоящего Соглашения срока становится общеизвестной, публичной иначе, чем в результате нарушения настоящего Соглашения;

4.1.2. Если Конфиденциальная информация раскрыта Передающей стороной третьим лицам без ограничений в ее использовании;

4.1.3. В случаях, когда раскрытие Конфиденциальной информации предусмотрено законодательством Российской Федерации.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. Стороны несут ответственность за нарушение обязательств по сохранению конфиденциальности в соответствии с действующим законодательством Российской Федерации и настоящим Соглашением.

6. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

6.1. Все споры и разногласия между Сторонами, связанные или вытекающие из Соглашения, разрешаются путем переговоров. Если переговоры не привели к согласию Сторон, спор подлежит рассмотрению в Арбитражном суде по месту нахождения Передающей стороны, в порядке, предусмотренном действующем законодательством Российской Федерации.

7. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

7.1. Настоящее Соглашение вступает в силу с даты его подписания обеими Сторонами. Условия настоящего Соглашения, ограничивающие распространение, передачу, использование и иные виды действий с Конфиденциальной информацией, полученной в соответствии с Соглашением, действуют в течение_____лет с даты последнего получения Получающей стороной Конфиденциальной информации, зафиксированной в Акте приема-передачи носителей конфиденциальной информации (Приложение 1 к Соглашению).

8. ПРОЧИЕ УСЛОВИЯ

8.1. Все уведомления и сообщения, направляемые Сторонами друг другу в соответствии с Соглашением или в связи с ним, должны быть совершены в письменной форме и переданы

заказным письмом, доставлены курьером или переданы уполномоченным представителем по следующим адреса

Передающая сторона:

Контактное лицо - _____

(телефон, e-mail)

Принимающая сторона:

Контактное лицо - _____

(телефон, e-mail)

Вся информация, передаваемая Получающей стороне согласно настоящему Соглашению, остается собственностью Передающей стороны.

8.2. Любые изменения и дополнения к Соглашению действительны при условии, что они совершены в письменной форме и подписаны уполномоченными представителями Сторон.

8.3. Настоящее Соглашение представляет собой исчерпывающую договоренность Сторон по предмету Соглашения. С момента подписания Соглашения все предыдущие переговоры и переписка по нему теряют силу.

8.4. Ни одна из Сторон не вправе передавать третьим лицам полностью или частично свои права и обязанности по Соглашению без предварительного письменного согласия другой Стороны.

8.5. В случае изменения действующего законодательства Российской Федерации недействительность или невозможность применения какой-либо части Соглашения не будет влиять на действительность или возможность исполнения другой части Соглашения, которая будет оставаться в силе и выполняться.

8.6. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

9. АДРЕСА И РЕКВИЗИТЫ СТОРОН

Передающая сторона:	**Получающая сторона:**
_____	_____
_____	_____
_____	_____
Должность	*Должность*
_____	_____
Подпись, инициалы, фамилия	*Подпись, инициалы, фамилия*
М.П.	М.П.

Приложение 5
к Соглашению о неразглашении и
защите конфиденциальной
информации от _____ № ___

АКТ №
приёма - передачи конфиденциальной информации

«_____» _____201__ г.

_____именуемый в дальнейшем «Передающая сторона», в лице _____ действующего на основании _____ с одной стороны,
и _____
именуемый в дальнейшем «Получающая сторона», в лице _____
действующего на основании _____с другой стороны,
составили настоящий Акт о нижеследующем:
Передающая сторона передала, а Получающая сторона приняла следующую Конфиденциальную информацию:

Наименование сведений и состав информации	**Название документа**	**Носитель информации**

Срок возврата носителей конфиденциальной информации или ее уничтожения.
« ___ » _____ 202_ г.

Передающая сторона:

_____
Должность

_____
Подпись, инициалы, фамилия

МП

Получающая сторона:

_____
Должность

_____
Подпись, инициалы, фамилия

МП

Приложение 6
к Соглашению о неразглашении и
защите конфиденциальной
информации от_____№_____

СПИСОК

Сотрудников _____

(наименование организации)

допущенных к конфиденциальной информации Передающей стороны

№ п/п	**Фамилия, имя, отчество**	**Должность (роль в проекте)**	**Роспись в ознакомлении с условиями Соглашения**

(должность) (подпись) (инициалы и фамилия руководителя Получающей стороны

« __ » _____ 202__ г.

М.П.