Утверждены
приказом и.о. Министра здравоохранения
Республики Казахстан
от «10» февраля 2014 года
№ 75

Регламент по обеспечению информационной безопасности

1. Общие положения

1. Регламент по обеспечению информационной безопасности (далее – регламент) разработан в соответствии с Государственной программой «Информационный Казахстан-2020» утвержденной Указом Президента Республики Казахстан от 8 января 2013 года № 464, а также в соответствии с Концепцией развития электронного здравоохранения Республики Казахстан на 2013-2020 годы утвержденной приказом Министра здравоохранения Республики Казахстан от 3 сентября 2013 года № 498.

2. Регламент устанавливает основные требования для обеспечения конфиденциальности персональных медицинских данных в процессах электронного здравоохранения, разграничению прав доступа к электронным информационным ресурсам, содержащим персональные медицинские данные, а также порядок работы и взаимодействия ответственных лиц по защите информации.

3. Настоящий регламент определяет требования к предоставлению доступа к информационным системам электронного здравоохранения, устанавливает ответственность пользователей, системных администраторов и лиц, ответственных за информационную безопасность, по исполнению и контролю указанных мероприятий.

4. Настоящий регламент определяет требования для выполнения процедур по предоставлению и прекращению доступа к информационным системам электронного здравоохранения.

5. В настоящем регламенте использованы ссылки на следующие нормативные правовые документы:

Закон Республики Казахстан от 11.01.2007 №217 – III «Об информатизации»;

Закон Республики Казахстан от 21 мая 2013 года 94 V «Закон о персональных данных и защите информации»;

Кодекс Республики Казахстан от 18 сентября 2009 года №193-IV «О здоровье народа и системе здравоохранения» с изменениями от 15 апреля 2013 года;

СТ РК ИСО/МЭК 27002-2009 – Информационные технологии. Средства обеспечения. Свод правил по управлению защитой информации;

СТ РК ИСО/МЭК 27001-2008 – Информационная технология. Методы и средства обеспечения. Системы управления информационной безопасностью. Требования;

СТ РК 34.005–2002 – Информационная технология. Основные термины и определения;

СТ РК 34.006–2002 – Информационная технология. Базы данных. Основные термины и определения;

СТ РК 34.007–2002 – Информационная технология. Телекоммуникационные сети. Основные термины и определения;

договор о неразглашении конфиденциальной информации;

Концепция развития электронного здравоохранения Республики Казахстан на 2013-2020 годы, утвержденная приказом Министра здравоохранения Республики Казахстан от 3 сентября2013 года № 498.

6. В настоящем регламенте использованы термины и понятия:

информационная система – совокупность информационных технологий, информационных сетей и средств их программно–технического обеспечения, предназначенных для реализации информационных процессов;

организация здравоохранения - юридическое лицо, осуществляющее деятельность в области здравоохранения;

организация – организации здравоохранения, либо третье лицо, уполномоченное в рамках договорных отношений, использующее информационные системы электронного здравоохранения;

пациент – физическое лицо, являющееся (являвшееся) потребителем медицинских услуг;

структурное подразделение информационной безопасности – структурное подразделение подведомственной организации Министерства здравоохранения Республики Казахстан, ответственное за обеспечение информационной безопасности;

отдел администрирования информационных систем – структурное подразделение подведомственной организации Министерства здравоохранения Республики Казахстан, ответственное за эксплуатацию и системно-техническое сопровождение информационных систем;

администратор информационной безопасности – сотрудник структурного подразделения информационной безопасности, ответственный за обеспечение информационной безопасности информационных систем электронного здравоохранения;

актив – материальная ценность предприятия или учреждения, которая составляет часть баланса этого предприятия;

несанкционированный доступ – доступ к информации в нарушение установленных в системе правил разграничения доступа;

объект – пассивный физический или информационный компонент системы (т.е. некий целостный набор информации, в который входят данные, объединенные общей темой, задачей, способом обработки и т.д.);

сервис – набор физических или программных компонентов информационной системы, объединенных функциональностью по предоставлению услуг по обработке, хранению или передаче информации;

системный администратор – сотрудник отдела администрирования информационных систем, отвечающий за администрирование и сопровождение информационных систем электронного здравоохранения;

средства вычислительной техники – аппаратные или программные средства, используемые для обработки, хранения и передачи информации;

системы предотвращения утечек информации - технические устройства (программные или программно-аппаратные), технологии предотвращения утечек конфиденциальной информации из информационной системы.

конфиденциальная информация – информация, поступающая и хранящаяся в информационных системах электронного здравоохранения, содержащая персональную информацию о здоровье или медицинские данные пациента;

персональная информация о здоровье – медицинские данные пациента, содержащие сведения анамнеза, заметки и другую информацию о состоянии здоровья, включая симптомы, диагнозы, препараты, результаты лабораторных анализов, основные показатели состояния организма, прививки и заключения по результатам диагностических обследований;

информационный ресурс – часть, модуль или отдельная подсистема информационной системы электронного здравоохранения, содержащая конфиденциальную информацию;

собственник информационной базы – лицо, реализующее в соответствии с действующим законодательством Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные медицинские данные, собственником является Министерство здравоохранения Республики Казахстан;

оператор информационной базы, содержащей персональные медицинские данные – государственный орган, и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;

личный кабинет пациента - доступ пациентов к собственным данным о здоровье и управление доступом к ним для медицинского персонала;

лог - файлы, в которых фиксируются все действия пользователя в информационной системе или ресурсе;

портал – совокупность интегрированных информационных ресурсов и информационных систем для просмотра персональных данных о здоровье;

обезличивание персональных данных – действия, в результате совершения которых определение принадлежности персональных данных в отношении конкретного пациента невозможно;

элемент электронной медицинской записи – это информация, описывающая конкретный клинический процесс в отношении субъекта оказания медицинской помощи, характеризующаяся конкретным автором,

отвечающим за содержимое информации, входящая в состав электронной медицинской записи и хранящаяся в организации возникновения.

период оказания медицинских услуг – временной интервал, в течение которого возникает один или более контактов между пациентом и поставщиком медицинских услуг в рамках полномочий на оказание медицинской помощи;

7. В настоящем регламенте использованы следующие обозначения и сокращения:

МЗ РК – Министерство здравоохранения Республики Казахстан;

СВТ – средства вычислительной техники;

ЭМЗ – электронная медицинская запись;

ЭЭМЗ – элемент электронной медицинской записи;

АРМ – автоматизированное рабочее место;

НУЦ – национальный удостоверяющий центр РК;

ЭЦП – электронно-цифровая подпись;

БД – базы данных;

ИБ – информационная безопасность;

ИС – информационная система;

НПА – нормативные правовые акты;

2. Правила предоставления доступа к информационным системам электронного здравоохранения

8. Персональная информация о здоровье относится к категории конфиденциальных электронных информационных данных, получение, обработка и использование которых, ограничивается целями, для которых она собирается. Информационные системы е-здравоохранения обеспечивают сохранность и ограничение доступа и использования персональной информации о здоровье только для целей оказания медицинской помощи и только на период оказания медицинских услуг. Представление сведений о состоянии здоровья от пациента для формирования электронных информационных данных здравоохранения осуществляется с письменного согласия пациента или его законного представителя.

9. Представление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается в следующих случаях:

в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;

при угрозе распространения заболеваний, представляющих опасность для окружающих;

по запросу органов дознания и предварительного следствия, прокурора, адвоката и (или) суда в связи с проведением расследования или судебного разбирательства;

при оказании медицинской помощи несовершеннолетнему или недееспособному лицу для информирования его законных представителей;

при наличии оснований полагать, что вред здоровью гражданина причинен в результате противоправных деяний.

10. Письменное согласие пациента оформляется по форме, согласно Приложению 1 к настоящему Регламенту.

11. В информационных системах медицинскому персоналу должны предоставляться персональные медицинские данные пациента для целей оказания медицинской помощи.

12. пациент или его законный представитель использует «Личный кабинет пациента» на портале для просмотра персональных данных о здоровье. Информация, которая будет доступна для просмотра пациенту, определяется лечащим врачом.

13. При использовании персональных данных о здоровье для проведения статистических, социологических, научных исследований необходимо использовать обезличенные данные. При использовании статистических и аналитических информационных систем сотрудниками Министерства здравоохранения Республики Казахстан, несвязанными непосредственно с оказанием медицинских услуг субъекту, для получения различных отчетов информационные системы также должны использовать обезличенные данные.

14. Сбор и обработка персональной информации о здоровье осуществляется только в случаях обеспечения их защиты. Защита персональной информации о здоровье осуществляется путем применения комплекса мер, в том числе правовых, организационных и технических, в целях:

реализации прав на неприкосновенность частной жизни, личную и семейную тайну;

обеспечения их целостности и сохранности;

соблюдения их конфиденциальности;

реализации права на доступ к ним;

предотвращения незаконного их сбора и обработки.

15. Информационные системы обеспечивают:

предотвращение несанкционированного доступа к персональным данным;

своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить, а также подозрение на несанкционированный доступ;

минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным.

16. Все изменения и дополнения к персональной информации о здоровье подтверждаются электронной цифровой подписью (далее - ЭЦП) медицинского работника. Все необходимые ключи и сертификаты для создания ЭЦП медицинские работники получают в Национальном удостоверяющем центре. Запись в логе, обеспечивающая аудит изменений и дополнений к персональной информации о здоровье, содержит описание произведенного изменения в персональной информации о здоровье, дату и время изменения, идентификатор медицинского работника, который произвел изменение, просматривал информацию, произвел копирование или распечатку.

17. Информационные системы обеспечивают конфигурирование настроек логирования случаев просмотра конфиденциальных данных на различных уровнях (модуля, медицинской организации, пользователя и т.д.).

3. Субъекты и объекты доступа

18. Субъектами доступа к информационным системам электронного здравоохранения и конфиденциальной информации являются:

пользователи - сотрудники организаций здравоохранения, имеющие допуск к информационным системам электронного здравоохранения и конфиденциальной информации;

администратор – сотрудник подведомственной организации Министерства здравоохранения Республики Казахстан, имеющий допуск к информационным системам электронного здравоохранения, осуществляющий администрирование и поддержание работоспособности информационных систем электронного здравоохранения и средств защиты информации;

администратор информационной безопасности - сотрудник подведомственной организации Министерства здравоохранения Республики Казахстан, ответственное лицо, осуществляющее контроль над выполнением требований по защите информации и исполнение организационно-распорядительных документов.

субъектом доступа может быть как лицо, так и процесс в информационной системе, запущенный от лица данного субъекта, а также стороннее лицо, которому по решению руководителя организации предоставлено разрешение для ознакомления или обработки конфиденциальной информации.

19. Объектами доступа являются информационные системы электронного здравоохранения, любые конфиденциальные информационные ресурсы на носителях информации и в памяти средств вычислительной техники.

20. Ответственность за организацию работ по доступу к

информационным системам электронного здравоохранения и защите конфиденциальной информации, контроль за эффективностью защиты информации возлагается на руководителя организации. Из состава сотрудников организации назначается администратор, имеющий административные права для управления информационными системами электронного здравоохранения.

21. Руководитель организации несет персональную ответственность за создание необходимых условий по предотвращению несанкционированного ознакомления с конфиденциальными информационными ресурсами и обеспечению их сохранности в организации, при обработке их с помощью СВТ.

22. Субъекты доступа, независимо от служебного положения должны строго выполнять требования данного регламента, принимать меры по предотвращению утечки конфиденциальной информации и целостности (модификации - это как частный случай целостности) конфиденциальной информации. Обязанности сотрудников организации по соблюдению требования настоящего регламента оговариваются при приеме на работу и закрепляются в трудовом договоре и должностных инструкциях или положениях о структурных подразделениях (в виде обязательства о неразглашении конфиденциальной информации).

23. Сотрудник может отказаться от дачи такой подписки, если средства обеспечения персонифицируемости электронной медицинской записи кажутся ему недостаточно надежными. Все конфликты, возникающие по этому поводу между сотрудником и администрацией, решаются в порядке, определенном законодательством Республики Казахстан.

24. С целью соблюдения принципа персональной ответственности за свои действия каждому субъекту доступа сопоставляется персональный уникальный идентификатор (логин, имя пользователя), под которым он регистрируется и работает в информационных системах электронного здравоохранения. Субъекту доступа в случае производственной необходимости могут быть сопоставлены несколько идентификаторов. Использование несколькими субъектами доступа одного и того же идентификатора (группового имени) для работы с информационными системами электронного здравоохранения запрещено. Передача субъектом доступа своей идентификационной информации (логина и пароля) другим лицам запрещена.

25. Средствами аутентификации субъектов доступа могут быть пароли, SMART-карты, идентификационные карты (магнитные или штрих-кодовые), USB-ключи и др. Для обеспечения прав доступа могут использоваться те же технические средства, что и для подписания электронной медицинской записи.

4. Предоставление прав доступа

26. Процедура регистрации (создания идентификатора и учетной записи) субъекта и предоставления ему (или изменения его) прав доступа к информационным системам электронного здравоохранения инициируется заявкой субъекта (Приложение №2). Заявка визируется руководителем организации, чем подтверждается производственная необходимость доступа (изменения прав доступа) данного субъекта и допуска данного лица к информационным системам электронного здравоохранения и конфиденциальной информации, необходимых для выполнения служебных обязанностей и решения им указанных задач. На основании заявки администратор производит необходимые операции по созданию (изменению, удалению) учетной записи, прав доступа и пароля.

27. Доступ к информационным системам электронного здравоохранения и конфиденциальной информации основывается на ролевом подходе, при регистрации субъекта организации ему назначается:

роль субъекта организации, которая строго ограничивает доступ субъекта к информационным системам электронного здравоохранения из других организаций;

роль профиля организации или подразделения, которая строго ограничивает доступ к конфиденциальной информациине относящейся к данному профилю организации или имеет статус «ограниченный доступ»;

роль служебного положения, которая разделена на несколько подролей в зависимости от уровня и статуса организации: руководитель организации - руководитель подразделения - лечащий врач - лаборант и т.д.

28. Роли доступа служебного положения:

персональная - предоставленная сотруднику лично (например, участковому врачу-терапевту данная роль предоставляет доступ к персональной информации о здоровье прикрепленного населения к территориальному участку, в соответствии с указанной процедурой как в пункте 13 или в соответствующей организационно-распорядительной документации);

должностная - предоставленная сотруднику в соответствии с занимаемой им должностью (лечащий врач, зав. отделением и др. в соответствии с указанной процедурой в пункте 13);

ситуационная - отвечающая ситуации (роли), в которой сотрудник исполняет свои обязанности (например, дежурный врач на время дежурства должен иметь больше прав, чем врач отделения; врач-консультант - только при проведении консультации или врач-лаборант при выполнении исследования может получать полный доступ ко всем ЭЭМЗ пациента в соответствии с указанной процедурой в пункте 13).

29. Права доступа могут распространяться на отдельные типы ЭЭМЗ или записи, относящиеся к определенному субъекту.

30. В основу распределения прав доступа должны быть положены требования к ведению бумажных медицинских документов, определенные

существующими нормативными документами, и принятая технология лечебно-диагностического процесса медицинской организации.

31. Права доступа пациента к ЭПЗ определены общими правами в соответствии с действующим законодательством Республики Казахстан, однако при этом обеспечивается конфиденциальность медицинских данных. Собственные ЭМЗ/ЭЭМЗ могут быть переданы субъекту в виде бумажных копий или в виде копий на электронных носителях (дискетах, CD и DVD дисках, флеш-картах и т.д.). При передаче пациенту бумажных или электронных копий ЭМЗ/ЭЭМЗ ответственность за обеспечение конфиденциальности возлагается на самого субъекта.

32. По решению руководства медицинской организации или этическим соображениям некоторые ЭМЗ/ЭЭМЗ могут быть закрыты лечащим врачом субъекта. При этом ответственность за соблюдение конституционных прав субъекта возлагается на руководство медицинской организации.

33. В установленном законодательством РК порядке, а также согласно правилам и документам, регламентирующим передачу ЭМЗ/ЭЭМЗ, данные ЭМЗ/ЭЭМЗ могут быть переданы независимым организациям (запросы правоохранительных органов, проведение экспертизы и т.д.). При передаче персональной информации о здоровье в электронной форме должны строго соблюдаться требования конфиденциальности в отношении медицинских данных субъекта. Передаваемые данные должны быть подписаны ЭЦП автора ЭМЗ/ЭЭМЗ или руководителя (доверенного лица) передающей организации.

34. При использовании ЭЦП для подписания ЭМЗ, подпись может охватывать всю информацию: ЭМЗ, все прикрепленные файлы и все элементы формализованных данных, а также ЭЦП может быть создана для каждой из составляющих частей ЭМЗ, прикрепленные файлы и элементы формализованных данных отдельно.

35. Для обеспечения требований информационной безопасности, а также проведения ревизии учетных записей, срок действия предоставления доступа не должен превышать 1 год (за исключением описанного в пункте 37 и 38). Данные ограничения устанавливаются администратором при создании учетной записи.

36. При регистрации (создания идентификатора и учетной записи) субъекта доступа, администратор в обязательном порядке включает запись всех действий пользователя (регистрация входа выхода, производимых действий), и др. Хранение информации о действиях пользователя должно храниться в течение 1 года, на внешних носителях в сейфе структурного подразделения информационной безопасности.

37. Деактивация учетной записи происходит на основании заявки подписанной руководителем организации, обходного листа предъявленного при увольнении сотрудником. Информация, созданная уволенным

пользователем, остается доступной для данной организации. В случае перемены места работы субъекта доступа организации, учетные данные не удаляются, а производится смена ролей в соответствии с вновь поданной заявкой.

38. Предоставление доступа субъектам доступа к конфиденциальным информационными ресурсами разрешается производить администратору. Субъекту доступа под роспись сообщается идентификатор, временный пароль, который должен быть заменен субъектом при первом входе в систему. Выдача доступа к информационным системам электронного здравоохранения регистрируется в журнале «Журнал регистрации пользователей и выдачи паролей» (Приложение 3).

39. Администратор имеет право:

приостанавливать оказание информационных услуг, доступ к конфиденциальной информации субъектам в случаях аварийных ситуаций, компрометации парольно-ключевой информации и по указанию руководителя организации;

проводить контроль исполнения требований по защите информации и технологии обработки конфиденциальной информации;

производить настройки на рабочих станциях субъектов доступа для обеспечения запрета на копирование конфиденциальной информации на внешние носители (USB, CD диски) и запрета на получение копии экрана (Print Screen).

40. Пользователи имеют право запрашивать информационные услуги, доступ к конфиденциальной информации и информацию о требованиях и правилах обработки конфиденциальной информации.

41. Предоставление прав доступа к информационным системам электронного здравоохранения и конфиденциальной информации сторонних информационных систем а также частных медицинских организаций, будет рассматриваться и регламентироваться в дополнительно разработанном регламенте «По предоставлению прав доступа частным медицинским организациям и сторонним информационным системам к информационным ресурсам МЗ РК», который будет разработан по мере необходимости.

5. Требования к парольной аутентификации

42. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей к информационным системам электронного здравоохранения, обрабатывающих конфиденциальную информацию и контроль за действиями субъектов возлагается на администратора.

43. Генерация временных паролей и изменение существующего пароля субъектом должны удовлетворять следующим требованиям:

длина пароля - не менее 8 символов;

в числе символов пароля обязательно должны присутствовать буквы в

верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

субъект не имеет права сообщать пароль доступа другому субъекту.

44. Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, несоответствующих данным требованиям, а также за разглашение парольно-ключевой информации.

45. При наличии технологической необходимости в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. допускать использование идентификаторов и паролей некоторых сотрудников в их отсутствие; идентификаторы и пароли предоставляются (ответственным сотрудником) с указания руководителя. При возвращении сотрудника к исполнению своих обязанностей, пароль изменяется в соответствии с вышеописанной процедурой. Сотрудник может потребовать у администратора полный список действий произведенных от его имени за время его отсутствия.

46. Полная плановая смена паролей субъектов должна проводиться не реже одного раза в месяц. Внеплановая смена паролей или учетных записей субъекта производится в случае прекращения его полномочий (увольнения, перехода на другую должность, в другое подразделение, сопровождаемое сменой допуска и прав доступа) или в случае компрометации пароля. Внеплановая смена паролей всех субъектов должна производиться в случае прекращения полномочий администратора.

47. Хранение сотрудником своих паролей (в печатном виде) и персональных идентификаторов допускается только в опечатанном конверте (Приложение 4) в сейфе структурного подразделения администрирования информационных систем.

6. Требования к обработке информации

48. Ввод конфиденциальной информации с печатных документов и других источников осуществляется только на автоматизированных рабочих местах, предназначенных для обработки конфиденциальной информации, сотрудниками, имеющими допуск к работе с конфиденциальной информацией. Создание конфиденциальных информационных ресурсов путем объединения (агрегирования) информации из нескольких конфиденциальных информационных ресурсов также является вводом и подлежит регистрации.

49. Конфиденциальные информационные ресурсы подлежат

хранению только на выделенных для этих целей серверах и системах, внешних носителях информации. Носители информации, используемые при создании резервных копий конфиденциальных информационных ресурсов, подлежат хранению так же, как и основные копии. Хранение конфиденциальных информационных ресурсов производится в течение срока, определяемого в соответствии с действующим законодательством Республики Казахстан. Носители информации, содержащие конфиденциальные информационные ресурсы, подлежат хранению в специально выделенном для этой цели сейфе.

50. В соответствии с требованиями информационной безопасности, данные, конфиденциальную информацию (в том числе персональные данные) следует хранить в БД в зашифрованном виде с тем, чтобы люди, имеющие доступ к БД (администраторы БД, хакеры и др.), не смогли прочитать эти данные. Данные должны быть видны только через приложения после того, как были проверены права доступа пользователя. Учитывая то, что шифрование базы данных в информационных системах электронного здравоохранения может в значительной мере повлиять на производительность систем, шифруется часть данных, по которым возможно определить субъект, к которому принадлежит медицинская информация.

51. Каналы передачи данных, по которым происходит передача конфиденциальной информации, а также ведется работа субъектов в информационных системах электронного здравоохранения, необходимо шифровать. Для всех каналов связи требуется использовать VPN– туннели. Создание и поддержку VPN– туннелей осуществляет подведомственная организация Министерства здравоохранения Республики Казахстан. Для порталов информационных систем электронного здравоохранения в обязательном порядке передача информации должна происходить с использованием HTTPS– протокола, данные меры полностью удовлетворяют требованиям информационной безопасности и позволяют защитить от перехвата трафика.

52. Уничтожение конфиденциальной информации и информационных ресурсов производится по истечении срока хранения (в соответствии с действующим законодательством Республики Казахстан).

53. Съемные носители конфиденциальной информации подлежат уничтожению при отсутствии необходимости их хранения. При уничтожении конфиденциальной информации составляется перечень всех носителей, содержащих данный информационных ресурсов, производится уничтожение данных информационных ресурсов и составляется акт установленной формы.

54. Для минимизации ущерба информационной безопасности необходимо использование систем предотвращения утечки информации, которое в свою очередь обеспечивает:

защиту интеллектуальной собственности;

предотвращение утечки персональных данных;

постоянный мониторинг информационных систем, персонала и использования ресурсов;

предотвращение неправомерного доступа к конфиденциальной информации;

выявление злоумышленников, лиц, занимающихся промышленным шпионажем, халатности персонала при работе с конфиденциальной информацией.

7. Обязанности субъектов доступа

55. Проверка правил разграничения доступа, прав и полномочий доступа к конфиденциальной информации информационных систем электронного здравоохранения, наличия носителей, содержащих конфиденциальную информацию, проводится не реже одного раза в год комиссией, назначаемой руководителем организации. Результаты проверки оформляются актом.

56. Все субъекты обязаны:

знать и выполнять требования настоящего Регламента;

хранить в тайне известную им конфиденциальную информацию, информировать своего непосредственного руководителя о фактах нарушения порядка обращения с конфиденциальными информационными ресурсами и носителями, и о попытках несанкционированного доступа к ним;

соблюдать правила пользования конфиденциальными ИР и носителями, порядок их обработки и хранения;

знакомиться только с той конфиденциальной информацией, к которой получен доступ в силу исполнения прямых служебных обязанностей;

использовать конфиденциальную информацию только в тех целях, для которых информация предоставлена субъектам доступа;

о допущенных нарушениях установленного порядка работы, учета и хранения конфиденциальной информации, а также о фактах разглашения конфиденциальной информации представлять письменные объяснения.

57. Субъектам доступа запрещается:

использовать конфиденциальную информацию при ведении переговоров по незащищенным каналам связи;

использовать конфиденциальную информацию в личных целях или в других целях, кроме как те, для которых информация предоставлена;

делать копии с конфиденциальных информационных ресурсов и носителей, а также использовать различные технические средства для их записи без разрешения руководителя организации;

работать с конфиденциальной информацией и носителями на дому;

выносить носители информации, содержащие конфиденциальную информацию, за пределы территории организации без разрешения руководителя организации;

сообщать устно или письменно кому бы то ни было (в том числе

сотрудникам) конфиденциальную информацию, если это не вызвано служебной необходимостью;

делать записи, расчеты и заметки, содержащие конфиденциальную информацию в личных тетрадях, блокнотах, на неучтенных носителях информации.

58. Администратору запрещается:

предоставлять доступ в нарушении правил разграничения доступа и требований по защите информации;

приостанавливать оказание информационных услуг, доступ к конфиденциальной информации без последующего незамедлительного уведомления субъекта доступа или руководителя подразделения сотрудника (при отсутствии возможности уведомления субъекта);

производить регистрацию конфиденциальных информационных ресурсов, ввод, прием, вывод конфиденциальной информации, передачу, запись и хранение конфиденциальных информационных ресурсов на СВТ, неоснащенных средствами защиты информации, при отключенных или некорректно работающих средствах защиты информации.

8. Ответственность субъектов доступа.

59. Все субъекты доступа несут персональную ответственность за корректность и соответствие организационно-распорядительным документам, проведения операций по ознакомлению, обработке конфиденциальной информации, простановке, снятию, шифрованию и расшифрованию, печать, ввод электронных документов (информационных ресурсов), за сохранение в тайне и исключение утраты, подмены и разглашение парольно-ключевой информации, печатных документов (в т. ч. черновики), полученные при выводе конфиденциальных информационных ресурсов. Ответственность субъектов доступа определяется действующим законодательством Республики Казахстан и нормативными правовыми актами Министерства здравоохранения Республики Казахстан.

9. Приложения

Приложение 1

Образец

Согласие на представление сведений о состоянии здоровья для формирования электронных информационных ресурсов здравоохранения

Настоящим Я,*(Ф.И.О),* ИИН_____ /законный представитель, *(Ф.И.О) в родительном падеже* , ИИН_____, действуя своей волей и в своем интересе, подтверждаю, что даю согласие на представление моей персональной информации о здоровье или медицинские данные, содержащие сведения анамнеза, заметки и другую информацию о состоянии моего здоровья, включая симптомы, диагнозы, препараты, результаты лабораторных анализов и лечения, основные показатели состояния организма, прививки и заключения по результатам диагностических обследований и др.

Настоящим подтверждаю, что ознакомлен с целями обработки моих персональных данных: доступ к моим персональным медицинским данным должен быть ограничен только для целей оказания мне медицинской помощи. Для проведения статистических, социологических, научных исследований данные о моем здоровье должны быть обезличены (обезличивание данных - действия, в результате совершения которых определение принадлежности персональных данных конкретному лицу становится невозможным).

Настоящее право (согласие) действует в течение 75 лет и может быть отозвано, если иное не установлено действующим законодательством Республики Казахстан.

Дата «___»_____20__г. _____ Подпись

Приложение 2
Образец

З А Я В К А
на регистрацию пользователя в
Информационной системе Министерства здравоохранения
Республики Казахстан

регистрация / изменение прав
(нужное подчеркнуть)

Прошу зарегистрировать _____

(Ф.И.О.- полностью)

С Инструкциями пользования по эксплуатации компьютерного оборудования и программного обеспечения ознакомлен и обязуюсь их выполнять _____

(подпись пользователя)

1.	Наименование организации	
2.	Адрес Организации	
3.	Отдел, должность	
4.	Фамилия и имя на английском языке	
5.	№ кабинета, № телефона	
6.	Наличие ЛВС ПК (IP)	
7.	Подключение к ИСМЗ	
8.	Тип доступа	
9.	Права доступа (чтение, полный доступ)	

Руководитель_____
_____
(указать отдел) (дата подачи заявки)
Согласовано:_____
Начальник отдела (непосредственный руководитель)
Согласовано:_____

Начальник отдела ОСА
Согласовано:_____
Начальник отдела ОИБ

Приложение 3
Образец

Журнал регистрации пользователей и выдачи паролей (название подразделения)

Таблица 1 - Список ответственных сотрудников за выдачу паролей к системам

№	ФИО	Должность	Номер телефона	Ответственность	Примечание

Таблица 2 - Реестр информационных ресурсов компонентов ЕИСЗ, к которым выдаются пароли

Наименование информационного ресурса	Место размещения информационного ресурса	Ф.И.О., телефон ответственного администратора

Таблица 3 - Журнал выдачи паролей

Название информационного ресурса	Дата и время выдачи.	Основание	Ф.И.О., телефон ответственного администратора	Ф.И.О., телефон пользователя, (выданное имя, права, email)	Примечание

Приложение 4
Образец

Конверт

1.	**Подразделение, должность**	
2.	**Ф.И.О.**	
3.	**№ кабинета, № телефона**	
4.	**Дата/Время**	