Утверждено
приказом № 22/1 от 04.01.2017 года
главного врача
КГП на ПХВ "Городская поликлиника №1" КГУ "УЗ акимата СКО"

Положение об информационной безопасности
КГП на ПХВ "Городская поликлиника №1" КГУ "Управление здравоохранения акимата СКО"

1. Общие положения

Положение об информационной безопасности КГП на ПХВ "Городская поликлиника №1" КГУ "УЗ акимата СКО" (далее по тексту - Положение) разработано в соответствии с Государственной программой «Информационный Казахстан-2020», утвержденной Указом Президента Республики Казахстан от 8 января 2013 года № 464, концепцией развития электронного здравоохранения Республики Казахстан на 2013-2020 годы, утвержденной приказом Министра здравоохранения Республики Казахстан от 3 сентября 2013 года № 498, а также в соответствии с Регламентом по обеспечению информационной безопасности, утвержденный приказом и.о. Министра здравоохранения РК от 10.02.2014 года №75.

Положение 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.

Настоящее Положение 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.

Требования Положения распространяются на всех работников КГП на ПХВ "Городская поликлиника №1" КГУ "УЗ акимата СКО" (Предприятие).

В настоящем Положении 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 ISO/IEC 27002-2015 Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации;

СТ РК ИСО/МЭК 27001-2015 - Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования;

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

Обозначения и сокращения, использованные в Положении:

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. Информационные системы/ресурсы Предприятия и порядок доступа к ним

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.

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.

Согласие пациента или его законного представителя оформляется письменно.

Электронные информационные ресурсы, содержащие сведения, не составляющие государственные секреты, но доступ, к которым ограничен законами Республики Казахстан либо их собственником или владельцем, являются конфиденциальными электронными информационными ресурсами.

Электронные информационные ресурсы, содержащие персональные данные, относятся к **категории конфиденциальных электронных информационных ресурсов**, сбор, обработка которых ограничиваются целями, для которых они собираются.

Медицинскому персоналу Предприятия в информационных системах предоставляются персональные медицинские данные пациента для целей оказания медицинской помощи.

При использовании персональных данных о здоровье для проведения статистических, социологических, научных исследований необходимо использовать обезличенные данные.

Информационные системы Предприятия 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.

3. Субъекты и объекты доступа

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

- пользователи – сотрудники Предприятия, имеющие допуск к информационным системам электронного здравоохранения и конфиденциальной информации, а также стороннее лицо, которому по разрешению руководителя/Главного врача Предприятия предоставлено разрешение для ознакомления или обработки конфиденциальной информации.

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

Главный врач Предприятия несет Ответственность за организацию работ по доступу к информационным системам электронного здравоохранения и защите конфиденциальной информации, контроль за эффективностью защиты информации возлагается на Главного врача Предприятия.

Приказом по Предприятию из состава сотрудников организации назначается администратор, имеющий административные права для управления информационными системами электронного здравоохранения.

Главный врач Предприятия 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.

4. Права и обязанности субъектов доступа

Пользователи информационных систем обязаны:

1) знать и выполнять требования настоящего Положения;
2) хранить в тайне известную им конфиденциальную информацию, информировать своего непосредственного руководителя о фактах нарушения порядка обращения с конфиденциальными ресурсами и носителями, и о попытке несанкционированного доступа к ним;
3) пользоваться конфиденциальными ИР и носителями, проводить обработку и хранение таким образом, чтобы не допустить утечки информации;
4) знакомиться только с той конфиденциальной информацией, к которой получен доступ в силу исполнения прямых служебных обязанностей;
5) использовать конфиденциальную информацию только в тех целях, для которых информация предоставлена субъектам доступа;
6) предоставлять письменные объяснения при нарушении требовании по работе, учету и хранению конфиденциальной информацией;
7) не использовать конфиденциальную информацию в следующих случаях:
   - при ведении переговоров по незащищенным каналам связи;
   - в личных целях или в других целях, кроме как те, для которых информация предоставлена;
   - делать копии с конфиденциальных ИР и носителей, а также использовать различные технические средства для их записи без разрешения руководителя Предприятия;
   - работать с конфиденциальной информацией и носителями на дому;
   - выносить носители информации за пределы территории Предприятия без разрешения руководителя Предприятия;
   - сообщать устно или письменно кому бы то ни было (в том числе сотрудникам) конфиденциальную информацию, если это не вызвано служебной необходимостью;
   - делать запись, расчеты и заметки, содержащие конфиденциальную информацию в личных тетрадях, блокнотах, на не учтенных носителях;
   - запрещается передавать свой и пользоваться чужим индивидуальным паролем при работе в информационной системе электронного здравоохранения Республика Казахстан.

Пользователи информационных систем имеют право:

1) пользоваться конфиденциальными ИР и носителями, проводить обработку и хранение;
2) использовать конфиденциальную информацию только в тех целях, для которых информация предоставлена субъектам;
3) сообщать устно или письменно конфиденциальную информацию, если это вызвано служебной необходимостью.

5. Ответственность субъектов доступа

За нарушение требований настоящего Положения о соблюдении на предприятии информационной безопасности субъекты доступа – пользователи несут дисциплинарную, административную и уголовную ответственность, предусмотренную действующим законодательством Республики Казахстан.