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

ИНСТРУКЦИЯ
по обеспечению сохранности коммерческой и служебной тайны КГП на ПХВ "Городская поликлиника №1" КГУ "УЗ акимата СКО"

1. Общие положения

Инструкция по обеспечению сохранности коммерческой и служебной тайны КГП на ПХВ "Городская поликлиника №1" КГУ "УЗ акимата СКО" (далее по тексту - Инструкция) разработана 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, с Регламентом по обеспечению информационной безопасности, утвержденный приказом и.о. Министра здравоохранения РК от 10.02.2014 года №75, а также в соответствии с Положением об информационной безопасности КГП на ПХВ "Городская поликлиника №1" КГУ "УЗ акимата СКО".

Инструкция устанавливает порядок допуска и работы персонала с информацией содержащей конфиденциальные персональные медицинские данные в процессах электронного здравоохранения, разграничения прав доступа к электронным информационным ресурсам, содержащим персональные медицинские данные, а также порядок работы и взаимодействия ответственных лиц по защите коммерческой и служебной тайны.

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), имеющих доступ к информационной системе «Единая точка авторизации» (ИС «ЕТА»).

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.

2. Порядок доступа к информационным системам

При приеме на работу персонал, работа которых связана с интеграцией с ИС ЕТА, подписывает Обязательство о неразглашении конфиденциальной информации (далее – Обязательство) по форме согласно Приложения № 1 к настоящей Инструкции. Наименование МО и наименование информационных систем, к которым предоставляется доступ в документе «Обязательство о неразглашении конфиденциальной информации» заполняется в электронном виде. Собственноручно заполняются пользователем только ФИО, подпись и дата заполнения.

В случае если пользователь имеет доступ к информационным системам, авторизация в которых проходит через ЕТА (Единая точка доступа), то Обязательство заполняется в соответствии с примером в Приложении 2. То есть в шапке указывается полное наименование («Единая точка доступа») + в скобках перечень порталов, в которых авторизуется пользователь посредством ЕТА.

Если пользователь имеет доступ к информационным системам, не входящим в ЕТА (ПС АПП, ЭРСБ, СУКМУ, ДКПН, БГ, ЭРОБ, ЕФИС, ХПН), то на каждую из систем заполняется отдельное Обязательство.

После этого ответственный работник Предприятия, назначенный приказом главного врача, подписанное принятым на работу сотрудником Обязательство предоставляет в РЦЭЗ МЗ РК для получения логина и пароля для входа в ИС ЕТА.

Полученные логин и пароль также являются конфиденциальной информацией и не подлежат разглашению и передаче третьим лицам.

Каждый сотрудник Предприятия, получивший логин и пароль для входа в ИС ЕТА обязан производить вход в систему только под своим именем, т.е. со своим логином и паролем.

3. Права и обязанности субъектов доступа

Пользователи информационных систем обязаны:

1) знать и выполнять требования Положения об информационной безопасности;

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.

4. Ответственность субъектов доступа

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

Приложение №1
к инструкции по обеспечению сохранности
коммерческой и служебной тайны

ОБЯЗАТЕЛЬСТВО

о неразглашении конфиденциальной информации.

Работника КГП на ПХВ "Городская поликлиника №1" КГУ "УЗ акимата СКО", участвующего в интеграции с РГП на ПХВ «Республиканский центр электронного здравоохранения» Министерства здравоохранения и социального развития Республики Казахстан (далее – РЦЭЗ МЗСР РК) с информационной системой «Единая точка авторизации» (АПП, РПН, АИС Поликлиника, СУМТ, СУР) (далее – ИС ЕТА)

Я, нижеподписавшийся, _____

_____ ФИО (полностью, собственноручно), в период участия в интеграции с РЦЭЗ МЗСР РК ИС ЕТА, обязуюсь:

1. Не разглашать информацию, составляющие служебную и/или иную тайну, охраняемую действующими законами, подзаконными актами и другими правовыми нормами Республики Казахстан (далее – сведения конфиденциального характера) и Министерства здравоохранения и социального развития Республики Казахстан (далее – Министерство), которые мне будут доведены или станут известны в связи с участием в интеграции с ИС ЕТА.

2. Не разглашать и не передавать третьим лицам данные, предоставленные для доступа к сервису ИС ЕТА.

3. Не разглашать информацию, которая содержится в материалах (решениях), полученных (принятых) в ходе заседаний по интеграции с ИС ЕТА. Информация, материалы, документы, презентации полученные в рамках работы являются сведениями конфиденциального характера.

4. Не передавать третьим лицам и не раскрывать сведения, составляющие сведения конфиденциального характера без решения руководства РЦЭЗ МЗСР РК.

5. Сохранять сведения конфиденциального характера юридических и физических лиц, с которыми буду взаимодействовать в ходе интеграции с ИС ЕТА.

6. В случае попыток посторонних лиц получить от меня вышеописанные сведения обязуюсь незамедлительно сообщить руководству РЦЭЗ МЗСР РК.

7. Я предупрежден, что за нарушение настоящего Обязательства, за утрату или неаккуратное хранение документов, содержащих служебную и/или коммерческую тайну, буду привлечен к ответственности, в соответствии с действующим законодательством Республики Казахстан.

_____ Подпись

_____ Дата

М.П.

Выписка из Закона РК «Об информатизации»

Глава 5. Электронные информационные ресурсы

Статья 32. Виды электронных информационных ресурсов

п.7 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;

Статья 36. Электронные информационные ресурсы, содержащие персональные данные

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

6. Не допускается использование электронных информационных ресурсов, содержащих персональные данные о физических лицах, в целях причинения имущественного и (или) морального вреда, ограничения реализации прав и свобод, гарантированных законами Республики Казахстан.

Глава 9. Защита объектов информатизации

Статья 53. Цели защиты объектов информатизации

1. Защитой объектов информатизации является реализация комплекса правовых, организационных и технических мероприятий, направленных на сохранность объектов информатизации, предотвращение неправомерного и (или) непреднамеренного доступа и (или) воздействия на них.

2. Защита объектов информатизации осуществляется в соответствии с законодательством Республики Казахстан и действующими на территории Республики Казахстан стандартами в целях:

1) обеспечения целостности и сохранности электронных информационных ресурсов;

2) обеспечения режима конфиденциальности электронных информационных ресурсов ограниченного доступа;

3) реализации права субъектов информатизации на доступ к электронным информационным ресурсам;

4) недопущения несанкционированного и (или) непреднамеренного доступа, утечки и иных действий в отношении электронных информационных ресурсов, а также несанкционированного и (или) непреднамеренного воздействия на объекты информационно-коммуникационной инфраструктуры;

5) недопущения нарушений функционирования объектов информационно-коммуникационной инфраструктуры и критически важных объектов информационно-коммуникационной инфраструктуры.

3. Иными несанкционированными и (или) непреднамеренными действиями в отношении объектов информатизации являются:

1) блокирование электронных информационных ресурсов и (или) объектов информационно-коммуникационной инфраструктуры, то есть совершение действий, приводящих к ограничению или закрытию доступа к

электронным информационным ресурсам и (или) объектам информационно-коммуникационной инфраструктуры;

2) несанкционированная и (или) непреднамеренная модификация объектов информатизации;

3) несанкционированное и (или) непреднамеренное копирование электронного информационного ресурса;

4) несанкционированное и (или) непреднамеренное уничтожение, утрата электронных информационных ресурсов;

5) использование программного обеспечения без разрешения правообладателя;

6) нарушение работы информационных систем и (или) программного обеспечения либо нарушение функционирования сети телекоммуникаций.

4. Защита информационных систем осуществляется согласно классу, присвоенному в соответствии с классификатором.

Выписка из Закона РК «О персональных данных и их защите»

Статья 11. Конфиденциальность персональных данных (пункт 2)

Лица, которым стали известны персональные данные ограниченного доступа в связи с профессиональной, служебной необходимостью, а также трудовыми отношениями, обязаны обеспечивать их конфиденциальность.

Статья 22. Обязанности собственника и (или) оператора, а также третьего лица по защите персональных данных

1. Собственник и (или) оператор, а также третье лицо обязаны принимать необходимые меры по защите персональных данных, обеспечивающие:

1) предотвращение несанкционированного доступа к персональным данным;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;

3) минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным.

Выписка из Кодекса РК «Об административных правонарушениях»

Статья 79. Нарушение законодательства Республики Казахстан о персональных данных и их защите

3. Несоблюдение собственником, оператором или третьим лицом мер по защите персональных данных – влечет штраф на физических лиц в размере ста, на должностных лиц, индивидуальных предпринимателей, юридических лиц, являющихся субъектами малого или среднего предпринимательства, или некоммерческими организациями, – в размере двухсот, на юридических лиц, являющихся субъектами крупного предпринимательства, – в размере трехсот месячных расчетных показателей.

Выписка из Уголовного Кодекса РК

Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа

1. Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем, – наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до шестидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья 223 Незаконные получение и разглашение сведений, составляющих коммерческую, банковскую тайну, а также информации, связанной с легализацией имущества» **(пункт 2).**

1. Незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца лицом, которому они были доверены по службе или работе, совершенное из корыстной или иной личной заинтересованности и причинившее крупный ущерб, – наказывается штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок.

Выписка из Гражданского кодекса Республики Казахстан

Глава 3. Объекты гражданских прав

Параграф 1. Общие положения

Статья 126. Служебная и коммерческая тайна

1. Гражданским законодательством защищается информация, составляющая служебную или коммерческую тайну, в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

2. Лица, незаконными методами получившие такую информацию, а также служащие вопреки трудовому договору или контрагенты вопреки гражданско-правовому договору, разгласившие служебную или коммерческую тайну, обязаны возместить причиненный ущерб.

Ознакомлен _____

(ФИО полностью, собственноручно)

_____ Подпись

_____ Дата

М. П.