«Утверждено»

Главный врач
КГП на ПХВ «Шарская городская больница»УЗ ВКО
_____Карсакбаев А.Б.
«__12.__» ноября 2018 года.

ИНСТРУКЦИЯ
по обеспечению сохранности коммерческой и служебной тайны КГП на ПХВ «Шарская городская больница» УЗ ВКО

1. Общие положения

Инструкция по обеспечению сохранности коммерческой и служебной тайны КГП на ПХВ «Шарская городская больница» УЗ ВКО (далее по тексту - Инстркуция) 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 «Жарминская центральная районная больница» УЗ ВКО.

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 «Жарминская центральная районная больница» УЗ ВКО (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, БСК, БГ), 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;

8) 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.