Государственное учреждение здравоохранения
«Пермский краевой госпиталь для ветеранов войн»

Утверждаю
Начальник госпиталя

_____В.А. Агафонов

«15» апреля 2011 г.

ПОЛОЖЕНИЕ

о защите персональных данных пациентов при пользовании персональным компьютером и ресурсами сети

ГУЗ «Пермский краевой госпиталь для ветеранов войн»

1. Общие положения

1.1. Целью настоящего положения является защита персональных данных пациентов путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.2. Настоящее положение определяет порядок получения, учета, обработки, накопления и хранения информации, содержащей сведения, отнесенные к персональным данным пациентов в Единой Корпоративной Сети Здравоохранения Пермского края (далее – Сеть), Региональной Информационной Аналитической Медицинской Системе и других программах, содержащих информацию о персональных данных пациентов (далее – Система), а также порядок работы системных администраторов и пользователей подключенного к сети компьютера, порядок распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, ответственность администраторов и пользователей подключенного к сети компьютера за неисполнение требований по защите персональных данных пациентов.

1.3. Пользователем подключенного к сети компьютера является работник ГУЗ «Пермский краевой госпиталь для ветеранов войн» (далее - Госпиталь), имеющий доступ к Сети, а также использующий в своей работе Систему (далее – Работник).

1.4. Персональными данными пациента является любая информация, относящаяся к конкретному пациенту, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

1.5. Персональные данные пациента являются строго конфиденциальными, любые лица, получившие к ним доступ, обязаны хранить эти данные в тайне, за исключением данных, относящихся к следующим категориям:

1.5.1. обезличенные персональные данные - данные, в отношении которых невозможно определить их принадлежность конкретному физическому лицу;

1.5.2. общедоступные персональные данные

1.6. Работники в своей деятельности руководствуются:

- Конституцией Российской Федерации от 12.12. 1993 года;
- Трудовым кодексом Российской Федерации от 30.12.2001 г. № 197-ФЗ;
- Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСТЭК РФ от 05.02.2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;
- иными нормативными правовыми актами, коллективным договором, локальными нормативными актами, содержащими нормы о защите персональных данных.

2. Порядок работы за компьютером.

2.1. При работе за компьютером работник обязуется:

2.1.1. использовать в работе предоставленные ему сетевые ресурсы в оговоренных в настоящем положении рамках, если иное не предусмотрено по согласованию с отделом информационных технологий. Системные администраторы вправе ограничивать доступ к

некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;
2.1.2. использовать электронную почту только для выполнения своих прямых служебных обязанностей;
2.1.3. использовать программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей;
2.1.1. приступить к работе в Системе только после назначения к выполнению указанной работы начальником соответствующего отдела, инструктажа и регистрации в отделе информационных технологий;
2.1.2. работать в Системе только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Изменения места работы, времени, программ и сетевых ресурсов допускается только с разрешения системного администратора;
2.1.3. вставлять и вынимать кабели, соединяющие системный блок с другими устройствами только при выключенном компьютере. Исключение составляют USB-устройства;
2.1.4. при входе в Систему использовать свои личные логин и пароль;
2.1.5. при авторизации в Системе использовать свою учетную запись;
2.1.6. по завершению рабочего дня выключить и обесточить компьютер;
2.1.7. блокировать или завершать программу по обработке персональных данных при оставлении рабочего места;
2.1.7. в случае нарушения правил пользования Системой, связанных с используемым компьютером, сообщить системному администратору, который проводит расследование причин данных нарушений, принимает меры к пресечению данных нарушений;
2.1.8. не разглашать известную ему конфиденциальную информацию необходимую для безопасной работы.

2.2. При работе за компьютером работнику запрещено:
2.2.1. самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере;
2.2.2. разрешать посторонним лицам пользоваться вверенным им компьютером;
2.2.3. использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования со специалистами отдела информационных технологий;
2.2.4. самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющих на работу сетевого оборудования и сетевых ресурсов;
2.2.5. повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;
2.2.6. самовольно подключать компьютер к Сети, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в Сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;
2.2.7. работать с каналоемкими ресурсами (video, audio, icq и др.) без согласования с системным администратором сети. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен;
2.2.8. использовать чужие имя и пароль при работе в системе;
2.2.9. подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям.

3. Ответственность за разглашение информации, связанной с персональными данными пациентов.

3.1. Лица, виновные в нарушении положений, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

4. Заключительные положения.

4.1. Настоящее положение вводится в действие на основании приказа начальника Госпиталя.

4.2. Работники считаются ознакомленными с настоящим положением с момента подписания Приложения № 1 к настоящему положению.