Утверждаю
Директор АНО «ЦБМ»
_____ _____ М.Г.
Скальная
«23» декабря 2011 г.

Политика Автономной некоммерческой организации «Центр биотической медицины» в отношении информационной безопасности персональных данных.

I. Введение

1.1. Настоящая Политика информационной безопасности АНО «ЦБМ» (далее – Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных пациентов Организации.

1.2. Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Настоящая Политика утверждена Приказом директора от «23» декабря 2011 г. № 46.

II. Общие положения

2.1. Целью настоящей Политики является обеспечение безопасности объектов защиты Организации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

2.2. Безопасность персональных данных достигается 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.

2.3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозу безопасности персональных данных.

III. Способы защиты персональных данных

3.1. Состав объектов защиты включает серверы СУБД и файл серверы, рабочие станции пользователей и аппаратные межсетевые экраны. Подсистема управления доступом реализована с помощью штатных средств обработки персональных данных с использованием парольной защиты рабочих станций и установкой на файл серверы и серверы СУБД операционной системы Microsoft Windows Server в редакции не ниже 2008.

3.2. Связь между подразделениями осуществляется по защищенным VPN-каналам с использованием протокола IPSec и шифрованием по алгоритму DES с длиной ключа не менее 56 бит.

3.3. Защита локальной сети организации от несанкционированных вторжений осуществляется штатными средствами аппаратных межсетевых экранов, допущенных к использованию на территории РФ, а также использованием антивирусного программного обеспечения.

3.4. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованное автоматизированное обновление антивирусных баз.

3.5. Амбулаторные карты, договоры и другие документы, содержащие данные о пациентах на бумажном носителе, обрабатываются специалистами отделов, в соответствии с Положением о разграничении прав доступа к обрабатываемым персональным данным.

3.6. Амбулаторные карты, договоры и другие документы, содержащие данные о пациентах на бумажном носителе хранятся в регистратуре Организации до момента оказания пациенту медицинской услуги в полном объеме. После этого амбулаторные карты передаются в архив, где хранятся в течение 25 лет в помещении, оборудованном системой пожаротушения.

3.7. В Помещение имеют доступ пользователи, имеющие право работать с амбулаторными картами пациентов, согласно Положению о разграничении прав доступа к обрабатываемым персональным данным.

IV. Пользователи ИСПДн

4.1. Данная Политика определяет основные категории пользователей, на основании чего произведена типизация пользователей информационной системы персональных данных, определен их уровень доступа и возможности: администратор и оператора рабочей станции.

4.2. Администратор обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных (ИСПД), а также полной информацией об используемых технических средствах и конфигурации информационной системы персональных данных.

4.3. Оператор рабочей станции, – сотрудник АНО «ЦБМ», осуществляющий обработку персональных данных (ПД), включая возможность их просмотра, ручной ввод ПД в систему ИСПД, формирование справок и отчетов по информации, полученной из ИСПД.

4.4. Оператор не имеет полномочий для управления системами обработки и защиты данных, обладает паролем, обеспечивающими доступ к ПД, необходимыми ему для выполнения своих функциональных обязанностей, располагает конфиденциальными данными, к которым имеет доступ.

V. Требования к персоналу по обеспечению защиты ИСПДн

5.1. Все сотрудники АНО «ЦБМ», являющиеся пользователями ИСПД, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПД.

5.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПД.

5.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПД.

5.4. Сотрудники АНО «ЦБМ» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение

имеют доступ посторонние лица, а именно производить блокирование рабочих станций при покидании рабочего места.

5.5. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

5.6. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Организации, третьим лицам.

5.7. При работе с ПД в ИСПД сотрудники Организации обязаны обеспечить отсутствие возможности просмотра ПД третьими лицами с мониторов рабочих станций.

5.8. При завершении работы с ИСПД сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

5.9. Сотрудники Организации должны быть проинформированы об угрозах нарушения режима безопасности ПД и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПД.

5.10. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПД, могущих повлечь за собой угрозы безопасности ПД, а также о выявленных ими событиях, затрагивающих безопасность ПД, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПД.

5.11. Требования настоящей Политики распространяются на всех сотрудников АНО «ЦБМ» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).