УТВЕРЖДАЮ

Главный врач
МБУЗ «Городская поликлиника №42
г. Ростова-на-Дону»

_____ И.А. Маслов

«12» января 2015 г.

ПОЛОЖЕНИЕ

ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
(в том числе персональных данных сотрудников)

В МБУЗ
«Городская поликлиника №42 г. Ростова-на-Дону»

ПОЛОЖЕНИЕ
по обеспечению безопасности конфиденциальной информации
(в том числе персональных данных работников)
МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону»

1. Под организацией обеспечения безопасности конфиденциальной информации (в том числе персональных данных работников) при ее обработке понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности конфиденциальной информации (в том числе персональных данных работников).

2. Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде носителей на бумажной, магнитной основе, в виде информационных массивов и баз данных в автоматизированных системах (АС).

3. Защищаемыми объектами информатизации являются:
- средства вычислительной техники;
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки конфиденциальной информации (в том числе персональных данных работников);
- носители на бумажной и магнитной основе (CD, НГМД, Flash)/

4. Защита информации должна осуществляться посредством выполнения комплекса мероприятий, отраженных в данном Положении, и применении (при необходимости) средств защиты информации по предотвращению утечки информации, воздействия на нее по техническим каналам, несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения.

5. При организации защиты информации конфиденциального характера (персональных данных) в МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» необходимо руководствоваться следующими нормативными документами:

- Федеральным Законом «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006г.
- Федеральным Законом «О персональных данных» № 152 от 27.07.2006г.
- «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным Постановлением Правительства РФ № 781 от 17.11.2007 г.
- Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- постановлениями Правительства РФ;
- другими нормативными документами ФСБ России, ФСТЭК (Гостехкомиссии) России по защите информации;
- приказами руководителя учреждения по вопросам защиты информации;
- эксплуатационно-технической документацией на объект информатизации ЛВС.

6. Обязанности по реализации необходимых организационных и технических мероприятий для защиты конфиденциальной информации (в том числе персональных данных работников) от неправомерного или случайного доступа к ней , уничтожения, изменения, блокирования, копирования, распространения конфиденциальной информации, а также иных неправомерных действий с ней, возлагается на Пользователя, допущенного к обработке конфиденциальной информации по приказу главного врача, на Ответственного по защите информации и Администратора безопасности конфиденциальной информации.

7. При обработке конфиденциальной информации (персональных данных работников) с использованием технических средств необходимо использовать только программное обеспечение, включенное в Перечень, утвержденный главным врачом. При установке нового программного обеспечения (ПО) необходимо пользоваться соответствующей Инструкцией по порядку установки нового общесистемного, прикладного и специального программного обеспечения. Устанавливаемое ПО должно удовлетворять требованиям, предъявляемым к программным продуктам для соответствующего класса защищенности Информационной системы персональных данных (ИСПДн).

8. Информацию конфиденциального характера (в том числе персональные данные работников) разрешается обрабатывать только на ПЭВМ, включенных в Перечень, утвержденный приказом главного врача. Технические средства, используемые для обработки конфиденциальной информации, должны быть опечатаны Ответственным по защите информации и Администратором безопасности информации.

9. К обработке конфиденциальной информации (в том числе персональных данных работников) допускаются лица, включенные в Список пользователей, допущенных к обработке информации конфиденциального характера, утвержденный приказом главного врача.

Допуск производится после проверки знания руководящих документов и практических навыков в работе. В случае необходимости внесение изменений в утвержденный Список пользователей (регистрация нового пользователя, расширение или сужение полномочий и прав доступа ранее зарегистрированного пользователя, исключение из Списка пользователей) осуществляется согласно Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн с оформлением соответствующей заявки. Новый пользователь допускается к обработке информации конфиденциального характера (в том числе персональных данных работников) только после ознакомления под роспись с соответствующими нормативными документами.

10. С целью предотвращения несанкционированного доступа к информации конфиденциального характера (в том числе персональным данным работников), обрабатываемой с помощью технических средств, необходимо использовать парольную защиту. Пользователи, использующие пароли, должны четко знать и строго соблюдать требования Инструкции по организации парольной защиты и своевременно сообщать Ответственному по защите информации и Администратору безопасности информации обо всех нештатных ситуациях, возникающих при работе с паролями.

11. Конфиденциальная информация (в том числе персональные данные работников), обрабатываемая с помощью технических средств, должна быть защищена от разрушающего воздействия компьютерных вирусов согласно Инструкции по организации антивирусной защиты. Порядок и периодичность антивирусного контроля и других необходимых антивирусных проверок определяется Администратором БИ.

12. По окончании обработки защищаемой информации с помощью технических средств, или при передаче управления другому лицу Пользователь обязан произвести стирание временных файлов на несъемных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПВЭМ.

13. Число и перечень абонентских пунктов (АП), используемых для обработки конфиденциальной информации (в том числе персональных данных работников), их взаимодействие с информационными сетями общего пользования (Сетями) осуществляется по приказу главного врача. К работе в качестве абонентов Сети допускаются Пользователи, ознакомленные с требованиями по взаимодействию с другими абонентами Сети и обеспечению при этом безопасности информации. Абоненты сети обязаны:

- знать порядок регистрации и взаимодействия в Сети;

- знать Инструкцию по обеспечению безопасности информации на АП;

- уметь пользоваться средствами антивирусной защиты;

- после окончания работы в Сети проверить свое рабочее место на наличие «вирусов».

Входящие и исходящие сообщения (файлы, письма, документы) учитываются в журналах несекретного делопроизводства (при необходимости).

Модификация конфигурации программного обеспечения АП, используемого для приема/передачи конфиденциальной информации (персональных данных работников), должна быть доступна только со стороны Администратора безопасности информации, либо, с его согласия, лицами, обслуживающими данное программное обеспечение.

14. При организации информационного взаимодействия в системе электронного документооборота конфиденциальной информации (персональных данных работников) необходимо использовать технические средства защиты информации - шифровальные (криптографические) (ЭЦП, VipNet) для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения., а также от иных неправомерных действий. Это необходимо выполнять как при передаче ПД по каналам связи (открытым или защищенным), так и при передаче ПД на внешних сменных носителях (НГМД, CD, Flash).При этом необходимо обеспечить надежное хранение ключей шифрования (ключевой документации), исключающее их хищение, подмену и уничтожение.

15. Все бумажные и магнитные носители конфиденциальной информации (CD, НГМД, Flash) должны храниться Пользователем в местах, недоступных для посторонних лиц.

16. При обнаружении нарушений системы защиты информации необходимо:

- немедленно прекратить работы по обработке информации;
- принять меры по устранению нарушения;
- организовать в установленном порядке расследование причин и условий появления нарушения с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;
- доложить непосредственному руководителю о вскрытых нарушениях и принятых мерах (при необходимости с привлечением Администратора БИ);
- возобновить обработку информации на объекте с разрешения непосредственного руководителя, предварительно согласовав свои действия с Администратором БИ, после устранения нарушения, условий его возникновения, проверки достаточности и эффективности принятых мер защиты.

17. При возникновении нештатных ситуаций Пользователь обязан действовать строго по Инструкции пользователю ОИ АРМ при действиях в нештатных ситуациях и Расчетом действия Пользователей конфиденциальной информации при возникновении пожара.

18. В случае возникновения неисправности технических средств АРМ необходимо провести дефектацию неисправного оборудования. Определение неисправного функционального блока или узла производится своими силами или с привлечением сторонних организаций, имеющих лицензию ФСТЭК России на право проведения ремонта.

19. При первом обращении пациента в поликлинику за медицинской помощью с 01.01.2010 г. единовременно оформлять письменное согласие на обработку его персональных данных в медицинском учреждении, которое должно храниться в Карте амбулаторного пациента.

20. При приеме на работу каждому работнику оформлять письменное согласие на обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование) и передачу его персональных данных, в том числе передачу третьим лицам – учреждениям и организациям, которым в соответствии с ФЗ «О персональных данных» МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» может поручить обработку персональных данных, или обязана представить персональные данные в соответствии с действующим законодательством РФ с целью выполнения обязанностей юридического лица.

Согласие работника действует с момента принятия его на работу в МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» и до истечения сроков, установленных действующим законодательством Российской Федерации.

21. Работники МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» должны быть ознакомлен с перечнем персональных данных, на обработку которых они дают согласие:
- фамилия, имя, отчество;
- дата и место рождения,
- гражданство;
- паспортные данные (серия, номер паспорта, кем и когда выдан), номера телефонов;
- место жительства/регистрации;
- сведения об образовании, в том числе наименование образовательного учреждения, специальность, квалификация;
- семейное положение;
- сведения о перемене фамилии:
- состав семьи;
- данные трудовой книжки (информация о трудовой деятельности до приема на работу в МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» (место работы, должность, период работы, причина увольнения);
- иные сведения о работнике, необходимые для корректного документального оформления правоотношений между работником и МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону».

22. Работники МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» должны быть ознакомлены с целями обработки их персональных данных:
- корректного документального оформления правоотношений между работником и МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону»;
- обеспечения выполнения работником своих обязанностей в процессе работы;
- предоставления информации в государственные органы Российской Федерации в порядке, предусмотренном действующим законодательством;

МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» гарантирует обработку персональных данных работников в строгом соответствии с действующим законодательством РФ и «Положением по обеспечению безопасности конфиденциальной информации (персональных данных работников)» МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону»;

23. Работники МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» имеют право на бесплатный свободный доступ к своим персональным данным, обрабатываемым в поликлинике.

24. Работники МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» несут ответственность за достоверность предоставленных сведений, а также должны сообщать в отдел кадров поликлиники обо всех изменениях их персональных данных в письменной форме (ксерокс документов) в срок, не превышающий 14 календарных дней с момента внесения изменений в соответствующие документы.

25. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности технических средств в МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону», необходимо проводить периодический (не реже одного раза в год) контроль состояния защиты информации, который заключается в следующем:

- анализ соблюдения нормативных и методических документов по защите информации, применяемых в учреждении;
- проверка работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- выполнения персоналом своих функциональных обязанностей в части защиты информации.

26. Эксплуатация объектов информатизации в МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» должна осуществляться в полном соответствии с утвержденной в поликлинике организационно-распорядительной документацией, Инструкциями по эксплуатации информационных систем персональных данных, настоящим Положением.

27. Все работники МБУЗ «Городская поликлиника №42 г. Ростова-на-Дону» должны быть ознакомлены под роспись с настоящим Положением.