Приложение 2 к приказу № 206/5 от « 29 » 08 2017г.

УТВЕРЖДАЮ
Главный врач ГБУЗ АО «Областная инфекционная клиническая больница им. А.М. Ничоги»
_____ А.М. Шишлонов
« 29 » 08 2017г.
(дата)

Политика информационной безопасности ГБУЗ АО «Областная инфекционная клиническая больница им. А.М. Ничоги»

1. Настоящая политика определяет цели и принципы обеспечения информационной безопасности государственного бюджетного учреждения здравоохранения Астраханской области «Областная инфекционная клиническая больница им. А.М. Ничоги» (далее – ГБУЗ АО «Областная инфекционная клиническая больница им. А.М. Ничоги», Учреждение).
2. Политика обязательна для исполнения всеми сотрудниками Учреждения, а также лицами, работающими с информацией, получаемой у Учреждения, в рамках заключенных договоров.
3. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.
4. Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности и улучшение деловой репутации Учреждения.
5. В Учреждении обрабатываются следующие категории информации ограниченного доступа (конфиденциальная информация):
   - Персональные данные работников;
   - Персональные данные субъектов персональных данных, не являющихся сотрудниками Учреждения (пациенты);
   - Служебная информация Учреждения, не содержащая персональных данных.

   Порядок обработки и защиты каждой категории сведений, закрепление ответственности за лицами, имеющими к ним доступ, в том числе санкции за невыполнение норм безопасности, регулирующих обработку и защиту конфиденциальной информации, закрепляются соответствующими локальными нормативными актами.

6. Обработка информации в Учреждении производится с соблюдением следующих принципов:
    - соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, а также целостности и доступности информации;
    - дифференцированный подход к обеспечению безопасности информации на основе ее классификации по степени ущерба от нарушений свойств безопасности;
    - ответственности и отчетности Учреждения перед гражданином (в том числе перед сотрудником Учреждения) за обработку сведений, содержащих его персональные данные;
    - учет и контроль всех этапов автоматизированной и неавтоматизированной обработки конфиденциальной информации;
    - осведомленность сотрудников Учреждения, осуществляющих обработку конфиденциальной информации, в вопросах информационной безопасности;
    - персональная ответственность сотрудников Учреждения за выполнение норм информационной безопасности;
    - использование принципа минимальных привилегий: доступ к конфиденциальной информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме; при этом разовый, либо постоянный допуски к конфиденциальной информации оформляются приказом главного врача.
7. Организация, предоставляющая Учреждению базы данных с персонифицированной информацией (реестры, перечни и т.п.), несет ответственность перед субъектом персональных данных за действия Учреждения согласно п.5. Ст.6 152-ФЗ «О персональных данных». Учреждение, в свою очередь, несет ответственность перед Организацией.
8. Меры защиты информации, выбираемые Учреждением, внедряются по результатам проведения оценки рисков информационной безопасности. Оценка рисков информационной безопасности проводится систематически, а также в случае значительных изменений в структуре Учреждения, и ее производственных процессах. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.