Приложение 1
к Приказу
от 15.04.2019 № 23 адм

ПОРЯДОК
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в БУЗОО «Клинический диагностический центр»

1. Общие положения

1.1. Настоящий Порядок осуществления внутреннего контроля соответствия обработки персональных данных (далее - ПДн) требованиям к защите ПДн в БУЗОО «Клинический диагностический центр» разработаны с учетом Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21 марта 2012г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящий Порядок определяет правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите ПДн и действуют постоянно.

2. Тематика внутреннего контроля

2.1. Тематика проверок обработки ПДн с использованием средств автоматизации:

– соответствие полномочий пользователя матрице доступа;

– соблюдение режима обработки информации (проверка идентификации и аутентификации пользователей, проверка работоспособности средств защиты информации и т.д.);

– соблюдение установленного режима защиты (проверка списков допущенных лиц, проверка наличия пломбы (наклейки) на корпусах ПЭВМ, металлических шкафах и (или) сейфах, соблюдение пользователями информационных систем парольной и антивирусной политики, соблюдение пользователями информационных систем правил работы со съемными носителями защищаемой информации и т.д.);

– соблюдение порядка доступа в помещения, в которых расположены элементы информационных систем;

– поддержание в актуальном состоянии нормативно-организационных документов (актуальность документов, регламентирующих деятельность по защите информации);

– контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационной системы обработки информации (проверка наличия на ПЭВМ нелицензионного программного обеспечения, игровых программ и другой посторонней информации, установленное ПО должно соответствовать Перечню разрешенного дня установки программного обеспечения);

– соблюдение порядка резервирования баз данных и хранения резервных копий;

– знание пользователями информационных систем, непосредственно осуществляющих обработку защищаемой информации, положений законодательства Российской Федерации о защите информации, в том числе требований к защите персональных данных, документов, определяющими политику БУЗОО «КДЦ» в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, и (или) обучение указанных сотрудников;

– знание пользователями информационных систем порядка действий во внештатных ситуациях;

– знание ответственными лицами порядка реагирования на обращения субъектов персональных данных о выполнении их законных прав в области защиты персональных данных.

– соблюдение ответственными за криптографические средства защиты информации правил работы с ними;

2.2. Тематика проверок обработки ПДн без использования средств автоматизации:

– хранение бумажных носителей с ПДн;

– доступ к бумажным носителям ПДн;

– доступ в помещения, где обрабатываются и хранятся бумажные носители с ПДн;

– знание ответственными лицами порядка реагирования на обращения субъектов персональных данных о выполнении их законных прав в области защиты персональных данных;

– знание пользователями информационных систем, непосредственно осуществляющих обработку защищаемой информации положений законодательства Российской Федерации о защите информации, в том числе требований к защите персональных данных, документов, определяющими политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

3. Правила проведения внутренних проверок

3.1. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям БУЗОО «КДЦ» организует проведение периодических проверок условий обработки ПДн, но не реже 1 раза в 3 года (постановление Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»).

3.2. Проверки осуществляются ответственным за организацию обработки ПДн или администратор безопасности информации (далее – Ответственный) либо комиссией, образуемой Главным врачом БУЗОО «КДЦ».

3.3. Внеплановые внутренние проверки проводятся по необходимости в соответствии с поручением Главного врача БУЗОО «КДЦ».

3.4. Проверки осуществляются согласно плану проведения проверок Ответственным либо комиссией непосредственно на месте обработки ПДн путем опроса, либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки ПДн.

3.5. Для каждой проверки составляется Протокол проведения внутренней проверки.

3.6. При выявлении в ходе проверки нарушений, Ответственным в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.7. Протоколы хранятся у Ответственного, проводившего проверку, в течение года после составления. Уничтожение Протоколов проводится Ответственным либо комиссией самостоятельно.

3.8. О результатах проверки и мерах, необходимых для устранения нарушений, Главному врачу докладывает Ответственный.