П Р А В И Л А

осуществления внутреннего контроля соответствия обработки персональных данных муниципального автономного учреждения здравоохранения «Детская городская клиническая больница №1» требованиям к защите персональных данных

1. Общие положения

1.1 Настоящий документ разработан в соответствие с нормативными документами в области защиты персональных данных и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) муниципального автономного учреждения здравоохранения «Детская городская клиническая больница №1» (далее – Учреждение).

1.2 Организационное и техническое обеспечение внутреннего контроля системы защиты информации возлагается на администратора информационной безопасности и на ответственного за информационную безопасность.

1.3 Изменения и дополнения к данному документу утверждаются в установленном порядке.

2. Правила внутреннего контроля

1. Проверки осуществляются администратором информационной безопасности и ответственным за информационную безопасность либо комиссией, образуемой распоряжением руководителя Учреждения. В проведении проверки не может участвовать сотрудник Учреждения, прямо или косвенно заинтересованный в её результатах.
2. Проверки соответствия обработки персональных данных установленным требованиям в Учреждении проводятся на основании утвержденного руководителем Учреждения плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).
3. Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.
4. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- осуществление мероприятий по обеспечению целостности персональных данных.

5. Администратор информационной безопасности и ответственный за информационную безопасность имеют право:

- запрашивать у сотрудников Учреждения информацию, необходимую для реализации полномочий;
- требовать от сотрудников, допущенных к обработке персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить руководителю Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

6. В отношении персональных данных, ставших известными администратору информационной безопасности и ответственному за информационную безопасность в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

7. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений составляется заключение.