Приложение N 10
к приказу ГБУЗ СО ПТД №3
№ 144-л от 15.04.2014г.

# Правила
## осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных в ГБУЗ СО ПТД №3

### 1. Общие положения

1.1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ СО ПТД №3 (далее – учреждение) устанавливаются процедуры (основания, порядок и формы) проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны в соответствии с Федеральными законами: от 27.07.2006г. N 152-ФЗ "О персональных данных", от 27.07.2006г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Постановлениями Правительства Российской Федерации: от 01.11.2012г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", от 21.03.2012г. N 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 и муниципальными органами" и другими нормативными правовыми актами.

1.3. Целью настоящих Правил является выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

1.4. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006г. N 152-ФЗ "О персональных данных".

### 2. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в учреждении организовывается проведение проверок условий обработки персональных данных.

2.2. Проверки условий обработки персональных данных на соответствие требованиям по защите персональных данных, в учреждении осуществляются Комиссией по проверке условий обработки персональных данных, назначенной приказом по учреждению.

Комиссия создается из сотрудников учреждения, ответственных за защиту информации и обработку персональных данных.

2.3. Проверки условий обработки персональных данных могут быть плановыми и внеплановыми, документарными и проводимыми в помещениях подразделений учреждения, в которых ведется обработка персональных данных.

2.4. При проведении проверок условий обработки персональных данных должен быть полностью, объективно и всесторонне исследован порядок обработки персональных данных и его соответствие требованиям обработки персональных данных, установленным в учреждении, а именно:

- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора персональных данных;

- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;

- отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

- 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;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

2.5. В случае выявления фактов:

- несоблюдения установленного порядка обработки персональных данных;

- несоблюдения условий хранения носителей персональных данных;

- использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

- нарушения заданного уровня безопасности персональных данных (конфиденциальность/целостность/доступность)

в обязательном порядке устанавливаются причины нарушения обработки персональных данных и наличие (отсутствие) вины.

2.6. Комиссия имеет право:

- запрашивать у сотрудников учреждения информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных лиц 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 главному врачу предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить главному врачу предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.7. В процессе проведения внутреннего контроля (проверок) соответствия обработки персональных данных требованиям к защите персональных данных разрабатываются меры, направленные на предотвращение негативных последствий выявленных нарушений.

2.8. В случаях выявления нарушений обработки персональных данных, требующих немедленного устранения, принимаются меры оперативного реагирования.

2.9. В отношении персональных данных, ставших известными Комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.