

ГАОУЗ «ДЕТСКАЯ ГОРОДСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №7»

ПРИКАЗ__

№ *2/а*

г. Казань

«*09*» *01* 20*24* г.

О внутреннем контроле соответствия обработки персональных данных в ГАОУЗ «Детская городская клиническая больница №7» требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21 марта 2012 г. №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», п р и к а з ы в а ю:

1. Создать комиссию по осуществлению внутреннего контроля соответствия обработки персональных данных в ГАОУЗ «Детская городская клиническая больница №7» требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (далее - Комиссия), в составе:

Председатель комиссии: Главный врач Галиуллин М.Я.

Заместитель председателя комиссии: Заместитель главного врача по организационно-методической работе Гатауллина Г.С.

Секретарь комиссии: Главная медицинская сестра Еникеева Л.Р.

2. Утвердить прилагаемые Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

3. Контроль за исполнением на стоящего приказа оставляю за собой.

Главный врач



М.Я. Галиуллин

УТВЕРЖДЕНА

приказом ГАУЗ «Детская городская клиническая больница №7»
от «09» 01 2014 г. № 14

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (далее - Правила), разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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» и определяют порядок и мероприятия, проводимые в рамках внутреннего контроля соответствия обработки персональных данных (далее - внутренний контроль) в ГАУЗ «Детская городская клиническая больница №7»

1.2. Внутренний контроль состоит из перечня мероприятий (внутренних проверок), выполнение которых позволяет оценить соответствие обработки персональных данных ГАУЗ «Детская городская клиническая больница №7» требованиям Федерального закона «О персональных данных» и принятым в соответствии с ним нормативным правовым актам. Политике в отношении обработки персональных данных в ГАУЗ «Детская городская клиническая больница №7» и иным локальным актам ГАУЗ «Детская городская клиническая больница №7», а также своевременно выявить и предотвратить нарушения законодательства Российской Федерации в сфере персональных данных.

1.3. В целях организации и осуществления внутреннего контроля в ГАУЗ «Детская городская клиническая больница №7» создается комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных в ГАУЗ «Детская городская клиническая больница №7» требованиям,

установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (далее - Комиссия). Численный и персональный состав Комиссии утверждается приказом ГАУЗ «Детская городская клиническая больница №7».

1.4. Внутренний контроль проводится не реже одного раза в год.

1.5. Настоящие Правила подлежат анализу и, при необходимости, пересмотру в случаях изменения законодательства Российской Федерации в отношении обработки персональных данных.

2. ФОРМИРОВАНИЕ ПЛАНА ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Проверки, осуществляемые в рамках внутреннего контроля, могут быть плановыми и внеплановыми.

2.2. Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся на основании подготовленного Комиссией ежегодного плана проведения внутренних проверок режима обработки и защиты персональных данных в ГАУЗ «Детская городская клиническая больница №7» (далее - План проведения внутренних проверок).

2.3. План проведения внутренних проверок должен содержать следующую информацию:

- наименование мероприятий (внутренних проверок);
- периодичность мероприятий (внутренних проверок);
- планируемые даты мероприятий (внутренних проверок);
- перечень лиц, ответственных за проведение мероприятий (внутренних проверок).

2.4. Ежегодный план проведения внутренних проверок утверждается локальным актом ГАУЗ «Детская городская клиническая больница №7».

2.5. В проведении мероприятий внутреннего контроля не могут участвовать сотрудники ГАУЗ «Детская городская клиническая больница №7», прямо или косвенно заинтересованные в их результатах.

3. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВЫХ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ

3.1. Внутренние проверки проводятся лицами, ответственными за проведение контрольных мероприятий согласно Плану проведения внутренних проверок, с привлечением при необходимости иных сотрудников

ГАУЗ «Детская городская клиническая больница №7» (в пределах их компетенции).

3.2. Внутренние проверки проводятся при непосредственном участии сотрудников ГАУЗ «Детская городская клиническая больница №7», осуществляющих обработку персональных данных.

3.3. Контроль соответствия условий обработки персональных данных осуществляется непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников ГАУЗ «Детская городская клиническая больница №7» участвующих в процессе обработки персональных данных.

3.4. При проведении внутреннего контроля должны быть 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;

- соблюдение мер по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- порядок и условия применения средств защиты информации;

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

- осуществление мероприятий по обеспечению целостности персональных данных;

- соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки персональных данных;

- наличие правовых оснований по сбору копий документов, содержащих персональные данные.

3.5. По результатам проведения внутренней проверки лицом, ответственным за проведение мероприятия согласно Плану проведения внутренних проверок, оформляется Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в ГАУЗ «Детская городская клиническая больница №7» (далее - Отчет о результатах проведения внутренней проверки). Форма Отчета о результатах проведения внутренней проверки приведена в ПРИЛОЖЕНИИ № 1 к настоящим Правилам.

3.6. В случае выявления нарушений соответствия обработки персональных данных установленным требованиям сведения о выявленных нарушениях фиксируются в Отчете о результатах проведения внутренней проверки.

3.7. Отчет о результатах проведения внутренней проверки предоставляется Комиссии лицом, ответственным за проведение мероприятия согласно Плану проведения внутренних проверок.

3.8. Для устранения нарушений, выявленных по результатам внутренних проверок Комиссия формирует План мероприятий по устранению нарушений, выявленных в результате проведения внутренней проверки режима обработки и защиты персональных данных в ГАУЗ «Детская городская клиническая больница №7» (далее - План мероприятий по устранению нарушений). Форма Плана мероприятий по устранению нарушений приведена в ПРИЛОЖЕНИИ № 2 к настоящим Правилам.

3.9. Комиссия определяет срок устранения каждого нарушения, выявленного в процессе проведения внутренней проверки.

3.10. По результатам определения мероприятий, необходимых для устранения выявленных нарушений, и сроков их выполнения, лица, причастные к выявленному нарушению, приступают к их устранению.

3.11. По результатам проведения мероприятий, включенных в ежегодный План проведения внутренних проверок. Комиссия ежегодно или по запросу руководителя ГАУЗ «Детская городская клиническая больница №7» формирует Отчет о выполнении плана проведения внутренних проверок режима обработки и защиты персональных данных в ГАУЗ «Детская городская клиническая больница №7» (далее - Отчет о выполнении плана проведения внутренних проверок). Форма Отчета о выполнении плана проведения внутренних проверок приведена в ПРИЛОЖЕНИИ № 3 к настоящим Правилам.

3.12. Отчет по результатам внутреннего контроля Комиссия направляет руководителю ГАУЗ «Детская городская клиническая больница №7»

3.13. При необходимости в ГАУЗ «Детская городская клиническая больница №7» дополнительно может вестись Журнал проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства, а также локальным актам ГАУЗ «Детская городская клиническая больница №7» (далее - Журнал проведения внутреннего контроля). Форма Журнала проведения внутреннего контроля приведена в ПРИЛОЖЕНИИ № 4 к настоящим Правилам.

3.14. Ответственность за своевременное ведение Журнала проведения внутреннего контроля возлагается на Комиссию.

4. ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВЫХ ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Внеплановые проверки соответствия обработки персональных данных установленным требованиям проводятся на основании поступившей информации о нарушении правил обработки персональных данных в ГАУЗ «Детская городская клиническая больница №7». Проведение внеплановой проверки организуется Комиссией в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

4.2. По результатам проведения внеплановой проверки также составляется Отчет о результатах проведения внутренней проверки.

5. ОТВЕТСТВЕННОСТЬ

5.1. Члены Комиссии и лица, ответственные за проведение мероприятий согласно Плану проведения внутренних проверок, обеспечивают конфиденциальность персональных данных, ставших известными им в ходе мероприятий внутреннего контроля.

5.2. Члены Комиссии и лица, ответственные за проведение мероприятий согласно Плану проведения внутренних проверок, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящих Правил.