Государственное бюджетное учреждение здравоохранения Республики Крым «Черноморская центральная районная больница» (ГБУЗ РК «Черноморская ЦРБ»)

ПРИКАЗ

28 февраля 2019 года **№ 85**

Черноморское

Об утверждении правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ»

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях обеспечения безопасности персональных данных при их обработке в ГБУЗ РК «Черноморская ЦРБ»

П Р И К А З Ы В А Ю :

1. Утвердить:
   1.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ» согласно приложению № 1.
   1.2. Состав комиссии по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ» согласно приложению № 2.
   1.3. Положение о комиссии по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ» согласно приложению № 3.
   1.4. План внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ» согласно приложению № 4.
2. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач Титов Е.Ю.

Приложение № 1
к приказу от 28.02.2019 № 85

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ»

1. Общие положения

1.1 Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в ГБУЗ РК «Черноморская ЦРБ» (далее - Оператор) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.2 Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и требованием Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 г. «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 организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях (отделениях) ГБУЗ РК «Черноморская ЦРБ».

1.3 Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.4 Проверки соответствия обработки персональных данных установленным требованиям в ГБУЗ РК «Черноморская ЦРБ» проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в ГБУЗ РК «Черноморская ЦРБ» письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

1.5 Проверки осуществляются комиссией, образуемой приказом главного врача ГБУЗ РК «Черноморская ЦРБ». В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в ее результатах. Состав Комиссии не менее 3-х человек, включая лицо, ответственное за организацию обработки персональных данных. Все члены комиссии при принятии решения обладают равными правами.

1.6 Проверка должна быть завершена не позднее чем через пятнадцать дней со дня принятия решения о ее проведении.

2. Порядок проведения внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Оператор организует проведение периодических проверок условий обработки персональных данных.

2.2. Внутренний контроль осуществляется не реже 1 раза в год. При необходимости контроль может проводиться чаще в соответствии с поручением ГБУЗ РК «Черноморская ЦРБ».

2.3. Ответственный либо комиссия проводит внутренний контроль непосредственно на месте обработки персональных данных, опрашивает работников, осуществляющих обработку персональных данных, осматривает рабочие места. Все работники обязаны по запросу контролирующих предъявить все материалы и документы, числящиеся за ними, дать устные или письменные объяснения по существу заданных вопросов.

2.4. По результатам проверки составляется Акт контроля соответствия обработки персональных данных по форме, приведённой в Приложении 1.

2.5. При выявлении нарушений в ходе проверки Ответственным либо Председателем комиссии:

- делается запись в Акте контроля соответствия обработки персональных данных о мероприятиях по устранению нарушений и сроках их исполнения;
- информация о нарушениях и о мерах для их устранения доводится до сведения главного врача ГБУЗ РК «Черноморская ЦРБ».

2.6. В ходе внутренней проверки контролирующие проводят:

- контроль соответствия обработки персональных данных требованиям законодательства, нормативных актов по вопросам обработки персональных данных;
- контроль выполнения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- проверку параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- анализ изменения угроз безопасности персональных данных в информационной системе Оператора, возникающих в ходе её эксплуатации;
- контроль наличия или отсутствия фактов несанкционированного доступа к персональным данным;
- контроль соблюдения работниками, допущенными к обработке персональных данных, локальных актов, регламентирующих обработку персональных данных Оператора.

3. Ответственность

3.1. За организацию проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства отвечает Ответственный либо Председатель комиссии.

3.2. Ответственность за соблюдение Правил возлагается на всех работников ГБУЗ РК «Черноморская ЦРБ», на которых распространяются правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

3.3 Главный врач ГБУЗ РК «Черноморская ЦРБ», назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

Приложение 1
К правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ»

АКТ
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ»

В соответствии с п. 4 ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в ГБУЗ РК «Черноморская ЦРБ» (далее — Оператор) проведен контроль соответствия обработки персональных данных следующим актам:

— Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, в том числе «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённому постановлением Правительства от 15 сентября 2008 г. № 687, и «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утверждённым постановлением Правительства от 1 ноября 2012 г. № 1119;

— Политике ГБУЗ РК «Черноморская ЦРБ» в отношении обработки персональных данных;

— Положению об обработке персональных данных в ГБУЗ РК «Черноморская ЦРБ»;

— иным локальным актам.

В результате проведения контроля выявлены нарушения:

_____
_____.

Меры по устранению нарушений:

_____
_____.

Срок устранения нарушений:

_____.

Ответственный за организацию обработки персональных данных

_____.

Предложения комиссии:

_____
_____.

Подписи членов комиссии:

_____ _____
(подпись) (фамилия, имя, отчество)

_____ _____
(подпись) (фамилия, имя, отчество)

Приложение № 2
к приказу от 28.02.2019 № 85

Состав комиссии
по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ»

Марцев Сергей Валерьевич	-	Заместитель главного врача по безопасности - председатель комиссии
Матвейкова Мария Александровна	-	Секретарь руководителя - секретарь комиссии
Бахарев Иван Геннадьевич	-	Техник-программист
Подорожняя Татьяна Васильевна	-	Начальник отдела кадров
Макурина Юлия Геннадьевна	-	Заместитель главного бухгалтера

Приложение № 3
к приказу от 28.02.2019 № 85

ПОЛОЖЕНИЕ
о комиссии по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ»

1. Общие положения

1.1. Положение о комиссии по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ» (далее - Комиссия) определяет функции, состав, полномочия и порядок функционирования комиссии по проведению внутреннего контроля соответствия обработки персональных данных в ГБУЗ РК «Черноморская ЦРБ» требованиям к защите персональных данных.

1.2. Комиссия вносит главному врачу ГБУЗ РК «Черноморская ЦРБ» предложения по вопросам обработки персональных данных в ГБУЗ РК «Черноморская ЦРБ».

2. Основные функции Комиссии

2.1. Комиссия изучает вопросы деятельности ГБУЗ РК «Черноморская ЦРБ», связанных с обработкой персональных данных и их защитой.

2.2. Комиссия осуществляет внутренний контроль соответствия обработки персональных данных в структурных подразделениях ГБУЗ РК «Черноморская ЦРБ» требованиям к защите персональных данных путем проведения проверок.

2.3. Доведение до структурных подразделений ГБУЗ РК «Черноморская ЦРБ» рекомендаций по организации сбора, обработки, хранения, передачи и защиты персональных данных.

3. Порядок работы Комиссии

3.1. Основной формой работы Комиссии является проверка.

3.2. Главный врач ГБУЗ РК «Черноморская ЦРБ» утверждает план проверки.

3.3. Председатель Комиссии осуществляет общее руководство деятельностью Комиссии, организует работу Комиссии, проводит заседания и осуществляет общий контроль за реализацией принятых Комиссией решений.

3.4. Секретарь Комиссии отвечает за подготовку проверок, оформляет акты внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных, контролирует выполнение рекомендаций Комиссии по результатам проверок, готовит отчеты о работе Комиссии.

3.5. Заседания Комиссии проводятся по мере необходимости, но не реже одного раза в год.

3.6. Материалы к обсуждению на заседаниях Комиссии готовятся секретарем Комиссии.

3.7. Заседание Комиссии считается правомочным, если на нем присутствует не менее половины общего числа ее членов.

3.8. Решения Комиссии принимаются простым большинством голосов присутствующих на заседании членов Комиссии. При равенстве голосов членов Комиссии

решающим является голос председателя Комиссии.

3.9. По результатам заседаний Комиссии оформляются протоколы заседаний Комиссии, которые подписываются председателем Комиссии и секретарем Комиссии.

3.10. По результатам осуществления внутреннего контроля соответствия обработки персональных данных в ГБУЗ РК «Черноморская ЦРБ» требованиям к защите персональных данных составляется акт внутреннего контроля соответствия обработки персональных данных ГБУЗ РК «Черноморская ЦРБ», который подписывается членами Комиссии в количестве не менее 3-х человек и утверждается председателем Комиссии, а в его отсутствие - заместителем председателя Комиссии.

4. Полномочия Комиссии

Комиссия имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на нее задач;
- привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы Комиссии, и выработки соответствующих рекомендаций и заключений;
- проводить проверку непосредственно на рабочих местах работников ГБУЗ РК «Черноморская ЦРБ»;
- получать доступ к информационным системам персональных данных в части касающейся ее полномочий;
– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;
- вносить главному врачу ГБУЗ РК «Черноморская ЦРБ» предложения об устранении нарушений в деятельности ГБУЗ РК «Черноморская ЦРБ» по вопросам, отнесенным к компетенции Комиссии.

5. Контроль за работой Комиссии

5.1. Комиссия подотчетна главному врачу ГБУЗ РК «Черноморская ЦРБ». Председатель Комиссии периодически, но не реже одного раза в год, отчитывается главному врачу ГБУЗ РК «Черноморская ЦРБ» об итогах работы Комиссии и реализации ее предложений и рекомендаций.

5.2 Итоги работы Комиссии отражаются в годовых отчетах, представляемых главному врачу ГБУЗ РК «Черноморская ЦРБ».

Приложение № 4
к приказу от 28.02.2019 № 85

ПЛАН
внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ РК «Черноморская ЦРБ»

№ п/п	Мероприятия	Периодичность	Исполнитель
1.	Контроль за соблюдением режима защиты персональных данных, политики в отношении обработки персональных данных, за выполнением работниками обязанностей по защите персональных данных, определенных в организационно-распорядительной документации	Постоянно	Администратор информационных систем персональных данных; Ответственный за обработку персональных данных
2.	Проверка актуальности перечня должностных лиц, имеющих право самостоятельного доступа в помещения, где обрабатываются или хранятся ПДн	Ежегодно/ после каждого изменения штатного расписания	Ответственный за обработку персональных данных
3.	Контроль выполнения требований по режиму доступа в защищаемые помещения и на автоматизированные рабочие места, на которых производится обработка персональных данных	Ежеквартально	Руководители подразделений Ответственный за обработку персональных данных
4.	Контроль соблюдения правил работы с носителями персональных данных	Ежеквартально	Руководители подразделений Ответственный за обработку персональных данных
5.	Контроль за соблюдением режима обработки персональных данных	Ежегодно	Комиссия по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
6.	Пересмотр и, при необходимости, корректировка учетных записей пользователей	Еженедельно	Администратор безопасности информационных систем персональных данных
7.	Проверка журналов средств защиты информации для своевременного обнаружения фактов несанкционированного доступа к персональным данным	Еженедельно	Администратор безопасности информационных систем персональных данных
8.	Контроль за выполнением антивирусной защиты, неизменностью настроек средств	Еженедельно	Администратор безопасности

	антивирусной защиты и своевременным обновлением антивирусных баз		информационных систем персональных данных
9.	Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации	Еженедельно	Администратор безопасности информационных систем персональных данных
10.	Контроль за обеспечением резервного копирования, проверка работоспособности резервных копий	Ежемесячно	Администратор безопасности информационных систем персональных данных
11.	Контроль состава технических средств и средств защиты информации, применяемых в информационных системах персональных данных	Ежемесячно	Администратор безопасности информационных систем персональных данных
12.	Обучение и повышение осведомленности работников в области защиты ПДн	Ежегодно	Лицо, ответственное за организацию обработки персональных данных
13.	Пересмотр организационно-распорядительной документации, регламентирующей порядок обработки персональных данных и требования по защите персональных данных, с учетом проводимых мероприятий по контролю	Ежегодно По факту изменения целей, или иного значимого аспекта информационной безопасности	Комиссия по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
14.	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных	Ежегодно	Лицо, ответственное за организацию обработки персональных данных Комиссия по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
15.	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	Раз в три года	Лицо, ответственное за организацию обработки персональных данных Администратор безопасности информационных систем персональных данных или Юридическое лицо, или индивидуальный предприниматель, имеющий лицензию на осуществление

			деятельности по технической защите конфиденциальной информации, привлеченные на договорной основе
16.	Контроль заведения и удаления учетных записей пользователей	Прием/увольнение работника	Администратор безопасности информационных систем персональных данных Начальник отдела кадров
17.	Контроль ознакомления вновь принимаемых работников с локальными нормативными актами, регламентирующими обработку ПДн	Ежегодно	Комиссия по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных