Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУЗ «Поликлиника №1» МЗ РСО-Алания

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года N 152-ФЗ «О персональных данных» и требованием Постановления Правительства Российской Федерации от 21 марта 2012 г. N 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 (отделах) ГБУЗ «Поликлиника №1» (далее – Поликлиника).

Правила обязательны для исполнения всеми должностными лицами Поликлиники, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Поликлиники осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях (отделах), а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных Поликлиники. Для участия в проведении контроля решением ответственного за организацию обработки персональных данных могут также привлекаться другие специалисты структурных подразделений (отделов) Поликлиники (по согласованию с их руководителями). В таких случаях контроль носит комплексный характер.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.
Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов министерства или нарушения требований по обработке и защите персональных данных.

Сроки проведения контрольных проверок доводятся руководителям проверяемых подразделений (отделов) не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений (отделов).

Периодичность и сроки проведения плановых проверок подразделений (отделов) Поликлиники устанавливаются планом, утверждённый Руководителем Поликлиники. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Для участия в проведении внутреннего контроля (проверки) ответственным за организацию обработки персональных данных заблаговременно назначаются соответствующие компетентные специалисты (далее – проверяющие лица). В случае проведения проверки комиссией также назначается её председатель.

Председатель комиссии (старший по проверке) подготавливает в адрес руководителя проверяемого структурного подразделения (отдела) распоряжение о проверке за подписью ответственного за организацию обработки персональных данных Поликлиники и перечень вопросов проверки (при необходимости). Председатель комиссии (старший по проверке) распределяет обязанности по проверке конкретных участков работы между проверяющими лицами.

Проверяющие лица инструктируются непосредственным главным врачом об особенностях работы в конкретном структурном подразделении (отделе) Поликлиники. За 3 – 4 дня до начала проверки они должны изучить материалы предыдущих проверок данного структурного подразделения (отдела), уточнить наличие в нем защищаемых ресурсов, сил и средств защиты персональных данных и их функционирование, а также особенности обработки и перечень обрабатываемых персональных данных в соответствующих структурных подразделениях (отделах).

В случае проведения проверки удалённых структурных подразделений (отделов) с выездом в служебную командировку лица, направляемые на проверку, должны оформить в установленном порядке необходимые командировочные документы.

3. Порядок проведения проверки

По прибытию в структурное подразделение (отдел) для проведения проверки председатель комиссии (старший по проверке) прибывает к руководителю проверяемого структурного подразделения (отдела)

Поликлиники, представляется ему и представляет других прибывших на проверку лиц. При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проверки, а также каких должностных лиц структурного подразделения (отдела) необходимо привлечь к проверке и какие объекты следует посетить. Допуск лиц, прибывших на проверку, к конкретным информационным ресурсам, охраняемым сведениям и техническим средствам производится руководителем структурного (отдела) подразделения на основании распоряжения о проверке. Подобный допуск должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать.

Руководителем структурного подразделения (отдела) принимаются необходимые меры для обеспечения работы комиссии по проверке и определяется должностное лицо структурного подразделения (отдела), ответственное за обеспечение работы комиссии.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в структурном подразделении (отделе) Поликлиники проверке подлежат следующие показатели:

1) В части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных и в положении о порядке обработки персональных данных Поликлиники, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствие с нормативными правовыми актами и локальными актами, принятыми в Поликлинике;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов сотрудниками (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов Поликлиники сотрудниками (служащими), имеющими доступ к персональным данным;

е) наличие лиц, назначенные ответственным за организацию обработки персональных данных в структурном подразделении (отделе), уровень их профессиональной подготовки и способность выполнить возложенные обязанности;

ж) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных;

з) соответствие схемы контролируемой зоны, перечня мест хранения материальных носителей, перечня лиц, допущенных к обработке персональных данных фактическому состоянию.

2) В части защиты персональных данных в информационных системах персональных данных (ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;- структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

б) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

в) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах ЭВТ;

г) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

д) соблюдение требований и правил антивирусной защиты ПЭВМ и программ;

е) контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

ж) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) В части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность классификации информационной системы;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о структурных подразделениях (отделах) Поликлиники, должностных инструкциях сотрудников (служащих) и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного Поликлиники и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

В ходе работы проверяющие лица должны принимать меры по устранению на месте отмечаемых нарушений и недостатков. Для этого с должностными лицами структурного подразделения (отдела), ответственными за конкретные участки работы, где отмечались недостатки, одновременно должны проводиться разъяснения требований руководящих документов и оказываться практическая помощь в правильной постановке работы.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

а) актом - при проведении проверки комиссией;

б) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах, как правило, на месте в структурном подразделении (отделе), подписывается председателем и членами комиссии (старшим по проверке), докладывается под роспись руководителю структурного подразделения (отдела) и представляется на утверждение (на доклад) ответственному за организацию обработки персональных данных Поликлиники. Один экземпляр документа высылается в структурное подразделение (отдел), которая прошла проверку.

В случае несогласия с выводами комиссии (проверяющих лиц) руководитель структурного подразделения (отдела) может выразить в письменном виде своё особое мнение (прилагается к акту и/или служебной записке).

Результаты проверок структурных подразделений (отделов) периодически обобщаются ответственным за организацию обработки персональных данных Поликлиники и доводятся до руководителей структурных подразделений (отделов). При необходимости принятия решений по результатам проверок структурных подразделений (отделов) на имя главного врача Поликлиники готовятся соответствующие служебные записки.

Заместитель руководителя _____ / А.Э.Калоева /

(подпись)