УТВЕРЖДАЮ
И.о. ректора СГМУ,
проректор по лечебной работе и последипломному образованию
_____ Л.Н. Горбатова
«20» 12 2012 г.

ИНСТРУКЦИЯ

по уничтожению персональных данных
государственного бюджетного образовательного учреждения
высшего профессионального образования
«Северный государственный медицинский университет»
Министерства здравоохранения Российской Федерации

Выпуск 1

Дата введения: 20.12. 2012 г.

Архангельск, 2012

	Должность	Фамилия И.О./ Подпись	Дата
Проект вносит	Начальник ОИ	Трифонов И.А.	20.11.12
Согласовано	Зав. юридической службой	Филипова О.И.	20.11.12
	Помощник ректора	Халезин А.С.	20.11.12
Экземпляр			

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет основные требования по обеспечению гарантированного уничтожения документов, содержащих персональные данные и утилизации машинных носителей информации не подлежащих дальнейшей эксплуатации.

1.2. Выполнение требований Инструкции является обязательным для всех работников ГБОУ ВПО СГМУ(г.Архангельск) Минздрава России (далее - Университет), допущенных к работе с персональными данными.

1.3. Настоящая инструкция разработана на основе нормативных актов, нормативно-методических документов по делопроизводству и архивному делу Российской Федерации, а также на основе организационно-распорядительных документов по обеспечению защиты персональных данных в Университете.

2. ВВЕДЕНИЕ

2.1. В ходе уничтожения документов на твердых и машинных носителях информации, содержащих персональные данные, угрозы их безопасности реализуются за счет:

- подмены документов, выделенных для уничтожения или изъятия из документов и дел отдельных частей (листов, фотографий, образцов печатей, росписей);
- ошибочного или умышленного выделения документов для уничтожения или фиктивное “уничтожение” ценных документов и дел;
- неполного уничтожения документов, дел и носителей, дающего возможность восстановить их текст;
- утраты (утери, кражи) документов и дел, выделенных для уничтожения;
- использования машинных носителей в своих личных целях.

2.2. Перечисленные факторы возникновения угроз становятся контролируемыми, при соблюдении следующих условий уничтожения документов, дел и носителей информации:

- коллегиальность принятия решения об уничтожении документов, дел и самого процесса уничтожения;
- документирование (актирование) подготовки к уничтожению и уничтожение документов и дел;
- внесение комиссией отметок об уничтожении в акт и учетные формы только после фактического уничтожения документов и дел.

3. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Технологическая схема уничтожения документов и машинных носителей информации, содержащих персональные данные, включает следующие процедуры:
- подготовку документов, дел и машинных носителей к уничтожению;
- оформление акта на уничтожение;
- уничтожение документов по акту;
- уничтожение документов без составления акта.

3.2. Процедура подготовки документов, дел и машинных носителей информации к уничтожению включает:
- выделение документов, дел и носителей информации, подлежащих уничтожению по различным причинам;
- получение письменного разрешения на уничтожение от руководителей структурных подразделений (направлений деятельности);
- систематизацию документов, дел и носителей информации по способам документирования факта уничтожения.

3.2.1. С оформлением акта уничтожаются документы и дела, включенные в номенклатуру дел, подлинники видео - аудиодокументов, проекты технических документов, черновики и проекты особо ценных документов, картотеки (журналы) учета конфиденциальных документов и другие подобные материалы.

3.2.2. Акт подписывают члены комиссии и утверждает руководитель Университета. С оформлением акта уничтожаются любые электронные документы, описи и учетные формы, находящиеся как в рабочем или архивном массивах компьютера, так и на магнитных носителях, хранимых вн ЭВМ.

3.2.3. При выполнении процедуры оформления акта на уничтожение документов проверяются следующие операции:
- включение отдельной позицией в акт каждого отобранного к уничтожению документа или дела (тома), документа или дела на магнитном или ином техническом носителе (Приложение №1);
- оформление в акте итоговой записи, подписание итоговой записи работниками, составившими акт;
- проверка наличия и комплектности документов и дел, включенных в акт;
- согласование акта с должностными лицами, подписание его членами комиссии и утверждение руководителем Университета.

3.2.4. В процедуру уничтожения документов по акту входят:
- проверка назначаемой комиссией наличия документов, дел (томов), магнитных и других носителей, включенных в акт, их комплектности и соответствия записям в акте;

- физическое уничтожение комиссией документов, дел, томов и носителей информации;
- внесение в акт (Приложение №2 и Приложение №3) и учетные формы документов и носителей информации записи об уничтожении, проставление росписи членов комиссии.

3.3. Фактическое уничтожение документов и дел с истекшим сроком хранения производится только после утверждения описей дел постоянного и длительного срока хранения за соответствующий период времени.

3.3.1. Подписывать акт и вносить отметки об уничтожении в учетные формы до фактического уничтожения конфиденциальных материалов не допускается.

3.4. Без составления акта уничтожаются испорченные бумажные и технические носители, черновики и проекты документов, внутренние описи документов, находящихся у исполнителя, и другие материалы, образовавшиеся при исполнении конфиденциальных документов.

3.4.1. В процедуру уничтожения документов и носителей информации без составления акта входят:
- разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя и второго сотрудника подразделения;
- накапливание остатков носителей в опечатываемом ящике (урне);
- физическое уничтожение остатков носителей несколькими сотрудниками подразделения;
- внесение отметок об уничтожении в учетные формы документов и носителей.

3.5. При выполнении процедур и операций уничтожения конфиденциальных документов, дел и носителей информации особое внимание обращается на коллегиальность осуществления этих действий и жесткое соблюдение последовательности процедур и технологии уничтожения.

3.6. После утверждения описей дел и документов постоянного срока хранения составляется акт о выделении дел и документов за соответствующий период к уничтожению, в который включаются отобранные постоянно действующей комиссией по защите информации для уничтожения дела, отдельные документы из дел и документы выделенного хранения. Акт может иметь форму, представленную в приложении № 1.

4. ПРОВЕРКА СРОКОВ ХРАНЕНИЯ ДОКУМЕНТОВ ПДн

4.1 При исполнении требований пункта 2 статьи 5 Федерального закона РФ «О персональных данных» от 27.07. 2006 г. № 152-ФЗ и проверке сроков хранения документов, подлежащих уничтожению, руководствоваться «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного

самоуправления и организаций, с указанием сроков хранения», утвержденный Приказом Министерства культуры Российской Федерации от 25.08.2010 № 558.

4.2. Пример сроков хранения документов, содержащих персональные данные:

- писем, резюме – 1год;
- локальных нормативных актов – 3года;
- расчетных ведомостей – 5 лет;
- личных карт, трудовых договоров - 75 лет

4.3. Персональные данные должны храниться в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки персональных данных, или утраты необходимости в их достижении.

5. ПОРЯДОК УНИЧТОЖЕНИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1 Уничтожение документов производится по истечении сроков их хранения, после проведения отбора документов, подлежащих передаче на постоянное хранение в государственные, районные, городские архивы, и утверждения описи этих документов постоянно действующей комиссией по защите информации Университета.

6. ПОРЯДОК УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

6.1. Списание машинных носителей данных производится специально назначаемой комиссией. Уничтожение планируется, отбираются носители с информацией, подлежащей уничтожению, определяется день, место и время уничтожения.

6.2. Носители информации, содержащие персональные данные, при списании должны быть либо физически уничтожены, либо должна быть осуществлена многократная (на физическом уровне) перезапись информации.

6.3. Следующая информация на носителях перед списанием или ремонтом должна быть удалена с помощью сертифицированных средств гарантированного удаления информации:

- персональные данные;
- конфиденциальная информация;

6.4. При отсутствии возможности гарантийного удаления информации на машинных носителях персональных данных, такие устройства уничтожаются методом механического разрушения.

6.5. Каждый случай уничтожения носителей конфиденциальной информации необходимо регистрировать. Уничтожение производилось специально назначенной комиссией, каждый из членов которой был обязан расписаться в акте уничтожения.

6.6. При уничтожении машинные носители данных снимаются с материального учета.

6.7. Уничтожение машинных носителей оформляется соответствующим актом.

7. МЕСТА ДЛЯ ФИЗИЧЕСКОГО УНИЧТОЖЕНИЯ ДОКУМЕНТОВ

Физическое уничтожение дел и документов производится в специально отведенных местах:

7.1. Оборудованное место на территории Университета - для сжигания дел и большого количества бумажных документов, фото и видео материалов.

7.2. Кабинет для ксерокопирования документов – для измельчения документов на бумажной основе.

7.3. Слесарная мастерская - для механического разрушения машинных носителей информации.

8. ОБЯЗАННОСТИ СОТРУДНИКОВ, РАБОТАЮЩИХ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ И ИХ ОТВЕТСТВЕННОСТЬ

8.1. Сотрудники Университета, допущенные к работе с документами, содержащие персональные данные обязаны:

- выполнять требования приказов, инструкций и положений по обеспечению защиты персональных данных;
- об утрате или недостаче документов, а также о причинах и условиях возможной утечки сведений, немедленно сообщать руководителю структурного подразделения и ответственному по безопасности Университета.
- соблюдать правила пользования документами, содержащих персональные данные.
- выполнять требования внутри объектного режима, исключающие возможность ознакомления с конфиденциальными документами посторонних

лиц, включая и своих сотрудников, не имеющих к указанным документам прямого отношения.

- не использовать машинные носители в своих личных целях;
- исключить использование ставшей известной конфиденциальной информации в свою личную пользу.

8.2. Решение о привлечении к ответственности принимается руководством Университета по предложению руководителя структурного подразделения.

8.3. В необходимых случаях для оценки нанесенного вреда Университету, либо для выяснения других существенных обстоятельств проводится служебное расследование.

ПРОТОКОЛ РЕГИСТРАЦИИ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ СГМУ С ДОКУМЕНТАМИ СМК

Целевая аудитория:

____

Наименование документов:

Ознакомление/обучение провел: ______________________________________

(ФИО, должность)

____

С документами СМК ознакомлен (а):

Дата	ФИО	Должность	Подпись