УТВЕРЖДАЮ

Директор больницы

_____ В.А.Дуботолкин

Положение о защите персональных данных
ОГБУЗ «Костромская областная клиническая больница»

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", иными нормативно-правовыми актами, действующими на территории Российской Федерации.
1.2. Положение определяет порядок работы сотрудников ОГБУЗ «Костромская областная клиническая больница» (далее – Учреждение) с персональными данными, а также порядок учета, сроки хранения, периодичность и способы уничтожения документов, машиночитаемых носителей, содержащих персональные данные и иную конфиденциальную информацию.

2. Работа с документами на бумажных носителях

2.1. Персональные данные при их обработке, должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков). При фиксации персональных данных на бумажных носителях не допускается фиксация на одном носителе персональных данных, цели обработки которых заведомо не совместимы.

2.2. Документы на бумажных носителях, содержащие персональные данные должны храниться в сейфе, либо закрытом помещении, исключающем несанкционированный доступ к ним (исключение составляют документы, обрабатываемые в настоящий момент).

2.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

2.4. В отношении документов, содержащих персональные данные, должны быть определены места хранения материальных носителей и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

2.5. В каждом подразделении Учреждения определяется сотрудник, несущий ответственность за соблюдение правил хранения документов, содержащих персональные данные.

2.6. Снятие копий, а также производство выписок из документов, содержащих персональные данные, запрещено, если это не обусловлено производственной необходимостью и противоречит требованиям, предъявляемым к Учреждению как к оператору персональных данных.

2.7. Сроки хранения документов на бумажных носителях, содержащих персональные данные, регламентируется соответствующими нормативными документами. В случае если существующая нормативная база не позволяет установить сроки хранения документа, сроки хранения должны быть определены внутренними распоряжениями по подразделениям и утверждены приказами главного врача.

2.8. Руководитель подразделения Учреждения, осуществляющего работу с персональными данными, обеспечивает обязательное хранение документов, указанных в приложениях № 1 и № 2.

3. Работа с машиночитаемыми носителями

3.1. Информация, содержащая персональные данные, хранимая в машиночитаемом виде:

№ п/п	Вид информации	Срок хранения	Действия по окончании срока хранения
3.1.1.	Резервная копия базы данных соответствующей ИС или АИС на CD-RW (DVD+RW) с указанием даты создания	До физического износа носителя	уничтожение
3.1.2.	Машиночитаемая версия сведений, содержащих персональные данные, в выходных формах ИС и АИС, необходимых для деятельности подразделений Учреждения	До срока, установленного нормативными документами, либо до минования надобности	уничтожение
3.1.3.	Машиночитаемые версии сведений, содержащих персональные данные, необходимые для деятельности Учреждения, поступившие от других организаций (частных лиц) в установленном порядке	До срока, установленного нормативными документами, либо до минования надобности	уничтожение
3.1.4.	Базы данных соответствующего комплекса средств автоматизации находящиеся на жестких дисках сервера и/или АРМ	До срока, установленного нормативными документами или до минования надобности; до выхода носителя из строя или его замены.	уничтожение БД за период, не подлежащий хранению; уничтожение БД на носителе, подлежащем замене
3.1.5.	Электронные версии документов, содержащих персональные данные, необходимые для осуществления производственной деятельности.	До срока, установленного нормативными документами, либо до минования надобности	уничтожение

3.2. Внешние машиночитаемые носители (не входящие в состав системного блока компьютера) с конфиденциальной информацией, указанной в п.п. 3.1.1., 3.1.2., 3.1.3., 3.1.4., 3.1.5. должны находиться в сейфе, либо в закрытом помещении ограниченного доступа, исключающем несанкционированный доступ к ним (кроме

формируемых, обрабатываемых или используемых в данный момент). Машиночитаемые носители, используемые для записи резервной копии базы данных (п. 3.1.1), могут использоваться многократно и уничтожаются в случае их физического износа.
3.3. Восстановление данных с резервной копии без согласования с начальником отдела информации запрещается.
3.4. Не допускается передача сведений, содержащих персональные данные, через сети общего пользования (Интернет) по незащищенным каналам связи.
3.5. Работа специалистов Учреждения, допущенных к работе с персональными данными в ИС и АИС допускается только как пользователя с ограниченными правами и только с теми ресурсами, на допуск к которым он наделен полномочиями, в соответствии со своим должностным регламентом, функциональными обязанностями и утвержденной матрицей доступа. Каждый специалист при входе в систему идентифицируется в соответствии с установленной учетной записью (логин, пароль).
3.5. Сотрудникам Учреждения, допущенным к работе с персональными данными, запрещены чтение и перенос на жесткие диски информации с дискет, компакт дисков, флэш носителей и т.п., запись информации с жесткого диска на внешние носители. При необходимости все эти операции выполняет ответственный сотрудник отдела, который имеет право осуществлять распечатку и копирование необходимой информации на жесткий диск ИС, допуск к которой предусмотрен утвержденной матрицей доступа к персональным данным и иной конфиденциальной информации, обрабатываемой в комплексах средств автоматизации ГУЗ «Костромская областная больница».

4. Режим работы в помещениях ИС и АИС ограниченного доступа.

4.1. Помещения, в которых размещены сервера (серверная) и АРМ сотрудников АСУ (согласно утвержденному списку), осуществляющих работу со сведениями, содержащими персональные данные, являются помещениями с ограниченным доступом.
4.2. В помещении, где размещены АРМ сотрудников отдела информации (согласно списку), кроме самих сотрудников допускается нахождение начальника отдела информации, курирующего заместителя главного врача и главного врача в присутствии ответственного сотрудника отдела информации, утвержденного приказом руководителя. При этом допуск работников к программно-техническим ресурсам, базам данных, документации осуществляется в установленном порядке в строгом соответствии с нормативными правовыми документами. В помещении серверной имеют право находиться системный администратор, начальник отдела информации, курирующий заместитель главного врача, либо лица их заменяющие; нахождение в серверной других сотрудников учреждения возможно при возникновении служебной необходимости в присутствии начальника отдела информации. Нахождение иных лиц в помещениях отдела информации ограниченного доступа запрещено.

4.3. Сотрудники сторонних организаций при необходимости проведения регламентных (ремонтных) работ допускаются в помещения отдела информации при предъявлении паспорта, в сроки, согласованные с администрацией ОГБУЗ «Костромская областная клиническая больница» в присутствии начальника отдела информации. Во время обработки конфиденциальной информации сотрудники сервисного центра могут быть допущены только в экстренных случаях по согласованию с начальником отдела информации при условии исключения несанкционированного доступа к персональным данным и иной конфиденциальной информации и контроля за порядком осуществления проводимых работ.

4.4. Сотрудникам отдела информации, допущенным к работе с персональными данными пациентов, в соответствии с п.4.2. запрещены чтение и перенос на жесткий диск информации с дискет, компакт дисков, флэш носителей и т.п., запись информации с жесткого диска на внешние носители, а также печать на принтере. При необходимости все эти операции выполняет ответственный работник отдела, имеющий право осуществлять распечатку и копирование необходимой информации.

4.5. По окончании рабочего дня все документы и машиночитаемые носители, содержащие конфиденциальную информацию, переносятся в скрытое от посторонних глаз место помещения ограниченного доступа. Помещение закрывается на ключ ответственным сотрудником, ключи он хранит при себе с исключением доступа к нему посторонних лиц.

4.6. Ключи от серверной начальник отдела информации хранит при себе, при этом доступ посторонних лиц к ключам должен быть исключен. Уборка помещений осуществляется в присутствии ответственного сотрудника отдела информации либо начальника отдела информации.

4.7. Перед началом работы ответственный сотрудник отдела информации обязан проверить целостность замка двери помещения. В случае обнаружения повреждений замков или утраты ключей ответственный работник незамедлительно сообщает об этом начальнику отдела информации.

4.8. Второй экземпляр ключа от помещения АРМ хранится у начальника отдела информации. Системные блоки АРМ должны быть опечатаны наклейками для контроля за обеспечением недопустимости несанкционированного вскрытия, доступа к жесткому диску в обход системы защиты, изменения технической конфигурации.

5. Учет и хранение машиночитаемых и бумажных носителей информации, содержащей персональные данные, созданных с использованием технических средств

5.1.Хранение документов и информационных ресурсов, созданных с использованием технических средств и содержащих персональные данные, осуществляется только на предварительно учтенных машиночитаемых и бумажных носителях. Учет указанных носителей информации исполнителем ведется в книге учета установленной формы (приложение № 2).

5.2. Учет носителей конфиденциальной информации осуществляет ответственный сотрудник подразделения непосредственно перед записью или распечаткой на него конфиденциальной информации. Учетный номер на диски CD-R, CD-RW, DVD+R, DVD+RW наносится маркером, обеспечивающим нестираемость надписи без физического повреждения диска. Учетный номер на бумажный носитель наносится шариковой ручкой или при распечатке на принтере.

5.3. Для учета бумажного носителя конфиденциальной информации используется следующая нумерация:

NNN – Б – XXX – DD.MM.YYYY

Где «NNN» – очередной порядковый номер учета бумажных носителей, начиная с номера 001; «XXX» - идентификатор подразделения, состоящий из трех первых букв наименования, «DD.MM.YYYY» - дата выполнения распечатки на бумажный носитель в формате число, месяц, год.

Например: 001-Б- БУХ-05.06.2007, затем 002-Б-БУХ-15.06.2007 и так далее.

Бумажный носитель может иметь несколько листов, которые нумеруются обычным порядком.

5.4. Для учета машиночитаемого носителя конфиденциальной информации используется следующая нумерация:

NNN – М – XXX – DD.MM.YYYY

Где «NNN» – очередной порядковый номер учета машиночитаемых носителей, начиная с номера 001; «XXX» - идентификатор подразделения, состоящий из трех первых букв наименования, «DD.MM.YYYY» - дата выполнения записи на машиночитаемый носитель в формате число, месяц, год.

Например: 001-М-АСУ-07.07.2007, затем 002-М-АСУ-27.07.2007 и так далее.

5.5. Испорченный при записи или распечатке предварительно учтенный носитель информации учитывается, хранится и уничтожается в установленном порядке.

6. Учет передаваемых и поступающих для обработки машиночитаемых и бумажных носителей персональных данных

6.1. Машиночитаемые и бумажные носители конфиденциальной информации, в установленном порядке поступившие в Учреждение для обработки от третьих лиц (организаций), а также передаваемые Учреждением третьим лицам (организациям), подлежат обязательному учету.

6.2. Учет указанных носителей информации исполнителем ведется в журнале установленной формы (приложение № 4). Листы журнала должны быть пронумерованы, сшиты и скреплены печатью ЛПУ.

6.3. Порядок проведения регистрации документов:

6.3.1. До начала работы с документами в правом верхнем углу титульного листа или на лицевой стороне машиночитаемого носителя проставляется надпись «Конфиденциально».

6.3.2. Ниже надписи «Конфиденциально» проставляется регистрационный номер следующего содержания:

К/-XXX-NN,

Где «NN» – очередной порядковый номер учета машиночитаемых носителей, начиная с номера 01; «XXX» - идентификатор подразделения, состоящий из трех первых букв наименования.

Например: К/-БУХ-01, затем К/-БУХ-02 и так далее.

В случае получения документа в количестве нескольких экземпляров их регистрация проводится как для разных документов.

7. Уничтожение документов и машиночитаемых носителей, содержащих конфиденциальную информацию

7.1. Уничтожение носителей, содержащих конфиденциальную информацию, по акту (приложение № 5) производит комиссия в составе не менее трех человек в сроки, указанные в п. 2 и п. 3 настоящего Положения. В акте указывается, что уничтожается и в каком количестве. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. Состав комиссии по уничтожению носителей, содержащих конфиденциальную информацию, определяется распоряжением главного врача. Комиссия по уничтожению носителей, содержащих конфиденциальную информацию, состоит из сотрудников, работающих в отделе ОГБУЗ «Костромская областная клиническая больница» на постоянной (штатной) основе.

7.2. Внешние машиночитаемые носители конфиденциальной информации уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации. Уничтожение информации, хранящейся на жестких магнитных дисках компьютера допускается производить устройством гарантированного уничтожения информации, хранящейся на жестких магнитных дисках компьютера.

7.3. Бумажные и прочие сгораемые носители уничтожаются путем сжигания или с помощью любых бумагорезательных машин, гарантирующих невозможность восстановления носителя.

7.4. Акт уничтожения носителей конфиденциальной информации хранится у руководителя соответствующего структурного подразделения Учреждения. Носители конфиденциальной информации с истекшим сроком хранения, поступившие из других организаций, уничтожаются по отдельному Акту. В этом случае Акт уничтожения носителей конфиденциальной информации составляется в двух экземплярах: первый экземпляр хранится у руководителя подразделения, второй в десятидневный срок передается учреждение, откуда поступил носитель информации.

7.5. Уничтожение носителей конфиденциальной информации осуществляется в десятидневный срок после истечения срока хранения.

8. Порядок и периодичность смены ключей и паролей доступа

8.1. Пароли доступа пользователя сотрудников меняются не реже одного раза в календарный год системным администратором (начальником отдела информации). Длина пароля должна быть не менее 5 символов и исключать простую комбинацию знаков.
8.2. Информация о пароле в составе: № ИС, № АРМ, дата, значение пароля, ФИО и роспись системного администратора хранится на учтенном бумажном носителе в помещении ограниченного доступа (серверной).
8.3. Кроме того, смена паролей осуществляется в случаях: принятия на работу нового системного администратора (начальника отдела информации); утраты ключа от помещений ограниченного доступа отдела информации; несанкционированного проникновения в помещения ограниченного доступа отдела информации; утраты ключа от двери помещения.

9. Особенности обеспечения безопасности информации ОГБУЗ «Костромская областная клиническая больница»

9.1. Помещения, в которых размещены сервера Учреждения и АРМ сотрудников отдела информации, осуществляющих работу со сведениями, содержащими персональные данные, оборудуются металлическими дверями и решетками на оконных проемах.
9.2. Выдача ключей (от помещения АРМ отдела) ответственным сотрудникам отдела информации (лицам, их заменяющим) производится после их утверждения приказом главного врача и регистрируется в Журнале установленной формы (приложение № 6). Возврат ключей от дверей осуществляется при увольнении, либо аннулирования доступа ответственного сотрудника отдела информации по другим причинам и регистрируется в названном Журнале. Ключи при возврате передаются начальнику отдела информации.
9.3. Выдача ключей от помещения серверной и помещения АРМ отдела производится начальнику отдела информации после подписания приказа о его назначении и регистрируется в Журнале установленной формы (приложение № 6). Возврат ключей от дверей осуществляется при увольнении начальника отдела АСУ и регистрируется в названном Журнале. Ключи при возврате передаются курирующему заместителю главного врача либо главному врачу.

10. Организация доступа к конфиденциальной информации

10.1. Доступ к работе с информацией, содержащей персональные данные (включение в список допущенных к работе с ПД), предоставляется сотрудникам подразделений Учреждения после ознакомления с Положениями о порядке обработки и защиты ПД и подписания соглашения о неразглашении персональных данных субъекта. Приказом главного врача в подразделении должен быть назначен ответственный сотрудник из числа допущенных к работе с ПД, который несет ответ-

ственность за доступ к персональным данным и за соблюдение установленных правил по их защите.
10.2. Список сотрудников, допущенных к работе с персональными данными, ведется руководителем подразделения. При изменении состава сотрудников, руководителем подразделения в трехдневный срок формируется новый список допущенных к работе с персональными данными и иной конфиденциальной информацией (при необходимости устанавливается ответственный сотрудник). При определении ответственного сотрудника его кандидатура утверждается приказом главного врача. Перед внесением в список лиц, допущенных к работе с конфиденциальной информацией, нового сотрудника руководитель соответствующего структурного подразделения (ответственный сотрудник) знакомит его под расписку с документами, регламентирующими работу с персональными данными в ОГБУЗ «Костромская областная клиническая больница» и оформляет необходимые для допуска к работе формы, которые визируются сотрудником. Расписки хранятся у руководителя подразделения. После оформления всех необходимых документов сотрудник считается допущенным к работе.
10.3. При смене ответственного сотрудника в период с дня окончания работы предыдущего ответственного сотрудника до начала работы нового, руководитель структурного подразделения несет полную ответственность за доступ к информации и соблюдению правил хранения и защиты персональных данных
10.4. При увольнении руководителя структурного подразделения его функции по защите персональных данных выполняет лицо, исполняющее обязанности руководителя. После заключения с новым руководителем подразделения трудового договора, он должен быть ознакомлен под расписку с документами, регламентирующими работу с персональными данными в ОГБУЗ «Костромская областная клиническая больница», оформить и завизировать необходимые для допуска к работе с персональными данными формы. После оформления всех необходимых документов сотрудник считается допущенным к работе руководителя подразделения.

11. Ответственность за несоблюдение требований по обеспечению безопасности информации

11.1. Специалисты Учреждения, допущенные к работе со сведениями содержащим персональные данные, допустившие нарушения при соблюдении требований безопасности информации, несут уголовную, административную, дисциплинарную ответственность в соответствии с действующим законодательством.
11.2. В случае выявления нарушений сотрудниками Учреждения, допущенными к работе с персональными данными, требований по безопасности информации, они несут материальную ответственность в соответствии с Положением об оплате труда сотрудников ОГБУЗ «Костромская областная клиническая больница».

Приложение № 1
к Положению о защите персональных данных
ОГБУЗ «Костромская областная клиническая
больница»

СПИСОК

нормативных документов обязательного хранения в подразделениях учреждения, осуществляющих работу со сведениями, содержащими персональные данные

1. Положение о порядке обработки персональных данных ОГБУЗ «Костромская областная клиническая больница» (с приложениями)

2. Положение о защите персональных данных ОГБУЗ «Костромская областная клиническая больница» (с приложениями)

4. Закон №152 ФЗ «О персональных данных»

Приложение № 2
к Положению о защите персональных данных
ОГБУЗ «Костромская областная клиническая больница»

СПИСОК

документов обязательного хранения в подразделениях учреждения, осуществляющих работу со сведениями, содержащими персональные данные

1. Список сотрудников подразделения, допущенных к работе с персональными данными.
2. Подписанные сотрудниками (согласно списка) соглашения о неразглашении персональных данных субъекта.
3. Приказ о назначении сотрудника, ответственного за соблюдение условий хранения документов, содержащие персональные данные.
4. Книга учета документов, содержащих персональные данные
5. Журнал регистрации носителей информации, содержащей персональные данные
6. Заявление-согласие субъекта (пациента) на обработку его персональных данных

Приложение № 3
к Положению о защите персональных данных
ОГБУЗ «Костромская областная клиническая больница»

Книга учета документов, содержащих персональные данные

№ п/п	Наименование документа, машиночитаемого носителя	Регистрационный номер	Количество листов (книга, брошюра)	Дата регистрации, подпись	№ Акта и дата уничтожения документа, информация о передаче документа (дата, подпись, ФИО принявшего документ)
1.					
2.					
3.					
4.					

Примечание. Данный журнал должен быть учтен, страницы пронумерованы, прошиты и опечатаны (опломбированы).

Приложение № 4
к Положению о защите персональных данных ОГБУЗ
«Костромская областная клиническая больница»

Ж У Р Н А Л

регистрации носителей информации,

содержащих персональные данные

Дата поступления	Регистрационный номер	Откуда поступил	Вид носителя	Кол-во носителей	№ и дата сопроводительного документа	Учетные номера носителей	Кому передан носитель	Дата передачи носителя	Дата и № акта уничтожения	Должность, Ф.И.О.	
										передавшего	получившего
1	2	3	4	5	6	7	8	9	10	11	12

Пояснение к заполнению Журнала

1. Указывается дата поступления или учета носителя.

2. Указывается учетный номер поступившего носителя.

3. Указывается наименование организации, направившей учтенный носитель.

4. Указывается вид носителя (бумага А4, CD-R, DVD-R).

5. Указывается количество носителей с одним учетным номером (количество листов, дисков).

6. Указывается номер и дата сопроводительного документа для полученных и переданных носителей.

7. Указывается учетный номер созданного носителя.

8. Указывается наименование организации, куда направлен созданный учетный носитель. В случае если носитель создан для использования в пределах Учреждения, указывается «Локальный». При порче носителя указывается «Испорчен при записи (распечатке)».

9. Указывается дата отправки носителя.

10. Указывается дата и номер акта уничтожения носителя.

11. Должность, фамилия имя отчество должностного лица, передавшего носитель.

12. Должность, фамилия имя отчество должностного лица, получившего носитель.

Приложение № 5
к Положению о защите персональных данных
ОГБУЗ «Костромская областная клиническая больница»

УТВЕРЖДАЮ

Директор ОГБУЗ «Костромская областная клиническая больница»

_____
(Ф.И.О., подпись)

«_____» _____ 200___ г.

А К Т № ___

уничтожения носителей персональных данных и иной конфиденциальной информации, обрабатываемой в ОГБУЗ «Костромская областная клиническая больница»

_____
(наименование избирательной комиссии)

«_____» _____ 20___ г.

Председатель комиссии _____
(ФИО), должность

Член комиссии _____
(ФИО), должность

Член комиссии _____
(ФИО), должность

составили настоящий акт в том, что « » 20 г. произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся на

_____

_____

_____

_____

_____

(наименование носителя, учетный номер, тип удаляемой конфиденциальной информации, персональных данных, способ уничтожения информации).

Председатель комиссии _____
(подпись)

Член комиссии _____
(подпись)

Член комиссии _____
(подпись)

Приложение № 6
к Положению о защите персональных данных
ОГБУЗ «Костромская областная клиническая больница»

Журнал учета выдачи ключей от помещений ограниченного доступа отдела информации ОГБУЗ «Костромская областная клиническая больница»

№ п/п	Дата выдачи	Наименование, учетный номер (при наличии)	Ф.И.О., подпись		Дата возврата	Ф.И.О., подпись	
			выдавшего	получившего		вернувшего	принявшего

Примечание. Страницы данного журнала должны быть пронумерованы, листы прошиты и опечатаны.