Приложение 9
к приказу ГУЗ «ГЦГП»
01.04.2022 № 134-ОД

ПОЛОЖЕНИЕ
о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные в государственном учреждении здравоохранения «Гродненская центральная городская поликлиника»

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Данное Положение устанавливает применяемые в Государственном учреждении здравоохранения «Гродненская центральная городская поликлиника» (далее - ГУЗ «ГЦГП») способы обеспечения безопасности при обработке персональных данных, которыми являются любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.

2. В соответствии с законодательством Республики Беларусь под персональными данными понимается любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное положение, образование, профессия, другая информация, необходимая ГУЗ «ГЦГП».

3. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения работниками и должностными лицами ГУЗ «ГЦГП», допущенными к обработке персональных данных, иными получившими доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

4. Обеспечение конфиденциальности персональных данных не требуется в случае:

обезличивания персональных данных (действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных);

для общедоступных персональных данных (персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов).

5. Перечни персональных данных и ответственных за хранение и обработку персональных данных утверждается положением об обработке и защите персональных данных в ГУЗ «ГЦГП» и приказом главного врача.

6. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных ГУЗ «ГЦГП» предоставляет работникам и должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

знакомит работника под роспись в с требованиями Политики оператора в отношении обработки персональных данных, с Положением об обработке и защите персональных данных, с Положением о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные и иными локальными правовыми актами ГУЗ «ГЦГП» в сфере обеспечения конфиденциальности и безопасности персональных данных;

представляет хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т. п.);

обучает правилам эксплуатации средств защиты информации;

проводит иные необходимые мероприятия.

7. Работникам и должностным лицам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. Без согласования с руководителем структурных подразделений, отделений, отдела кадров, бухгалтерии, планово-экономического отдела, юридической службы, регистратуры, формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

8. Работники и должностные лица ГУЗ «ГЦГП», работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с исполнением своих трудовых обязанностей. С ними в обязательном порядке проводится инструктаж и ознакомление с нормативным правовыми актами под роспись о неразглашении персональных данных в журнале регистрации инструктажа. Приложение 1.

9. При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с исполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

10. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством Республики Беларусь, Политикой оператора в отношении обработки персональных данных и иными локальными правовыми актами ГУЗ «ГЦГП» в сфере обеспечения конфиденциальности и безопасности персональных данных.

11. Запрещается передача персональных данных по телефону, факсу, электронной почте, за исключением случаев, установленных

законодательством и действующими в ГУЗ «ГЦГП» локальными правовыми актами.

12.Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

13. Работники и должностные лица ГУЗ «ГЦГП», работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, ключей от сейфов (хранилищ) личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

14. Работники и должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Республики Беларусь.

15. Отсутствие контроля со стороны ГУЗ «ГЦГП» за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством Республики Беларусь ответственности.

ГЛАВА 2. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

16. Обработка персональных данных, в том числе содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такая обработка осуществляется при непосредственном участии человека.

17. Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:

определяет места хранения персональных данных (материальных носителей);

осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

информирует лиц, осуществляющих обработку персональных данных без использования средств автоматизации, о перечне обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

организует раздельное, то есть не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, USB флеш-накопителей и пр.), обработка которых осуществляется в различных целях.

18. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

19. При несовместимости целей обработки персональных данных руководитель структурного подразделения должен обеспечить раздельную обработку персональных данных.

20. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, должно производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (уничтожение бумажных документов в соответствии с Главой 16 «Уничтожение документов с истекшими сроками хранения» инструкции по делопроизводству в государственных органах и иных организациях», утвержденной постановлением министерства юстиции Республики Беларусь т 19.01.2009 № 4.

Составляется опись документов на уничтожение, передается архивариусу ГУЗ «ГЦГП», который оформляет акт на уничтожение документов, передает заведующему хозяйством и далее такие документы утилизируются в спецавтохозяйстве.

21. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе.

ГЛАВА 3.ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

22. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в компьютерной сети (далее – КС) в автоматизированных программах и базах данных ГУЗ «ГЦГП». Приложение 2.

Безопасность персональных данных при их обработке в КС обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в КС информационные технологии.

Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Республики Беларусь требованиям, обеспечивающим защиту информации.

23. Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется при наличии паролей доступа.

24. Работа с персональными данными в КС обеспечивает сохранность носителей персональных данных и средств защиты информации, а также исключает возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

25. Компьютеры и электронные папки, в которых содержатся файлы с персональными данными работников ГУЗ «ГЦГП», для каждого пользователя защищены индивидуальными паролями доступа в отделе кадров, планово-экономическом отделе, бухгалтерии, юридической службе, службе охраны труда, отделе автоматизированных систем управления, технической службе и др.

26. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.

27. При обработке персональных данных в КС пользователями должно быть обеспечено:

использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

28. При обработке персональных данных в КС разработчиками и администраторами информационных систем обеспечивается:

обучение лиц, использующих средства защиты информации, применяемые в КС, правилам работы с ними;

учет права доступа и паролей доступа работников, допущенных к работе с персональными данными в КС, осуществляется в журнале Приложение 3;

учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

описание системы защиты персональных данных.

29. Специфические требования по защите персональных данных в отдельных автоматизированных системах ГУЗ «ГЦГП» определяются утвержденными в установленном порядке инструкциями по их использованию и эксплуатации.

ГЛАВА 4. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТВЕРДЫМИ КОПИЯМИ И ИХ УТИЛИЗАЦИИ

30. Все съемные носители, которые используются для передачи информации, содержащие персональные данные, подлежат учету. Каждому съемному носителю присваивается уникальный учетный номер.

31. Учет носителей, проверку их работоспособности осуществляют сотрудники отдела АСУ. При проверке носителя в присутствии материально ответственного лица при необходимости производится его очистка. Носитель подлежит проверке не реже 1 раза в год. Учет ведется в журнале регистрации носителей информации. Приложение 4.

Журнал хранится в отделе АСУ. В журнал заносится выдаваемый уникальный номер, ФИО ответственного лица, дата начала и окончания регистрации. Уникальный номер в качестве наклейки или этикетки крепится на носитель информации.

32. Каждый факт передачи информации с помощью съемных носителей должен регистрироваться в журнале регистрации передач информации, содержащей личные данные, в другие организации. Приложение 5.

Журнал ведется в каждом структурном подразделении. После передачи информации, она должна быть удалена со съемного носителя. Ответственность за сохранность информации во время передачи несет сотрудник, указываемый в журнале регистрации, ответственность за сохранность съемного носителя и за содержащуюся на нем информацию во все другое время несет материально ответственное лицо.

33. При работе со съемными носителями, содержащими персональные данные, запрещается:

хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах либо оставлять их без присмотра или передавать на хранение другим лицам;

выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

34. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения ГУЗ «ГЦГП».

35. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено главному врачу или заместителю главного врача, ответственному за организацию работы с персональными данными в ГУЗ «ГЦГП».

На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета.

Приложение 1

Журнал
регистрации инструктажа по работе с персональными данными
в ГУЗ «Гродненская центральная городская поликлиника»

№№ п/п	Дата проведения инструктажа	Фамилия, имя, отчество, прошедшего инструктаж по работе с персональными данными	Занимаемая должность, профессия инструктируемо	Название документов, дата и номер, по которым проведен инструктаж	Подпись, лица, прошедшего инструктажа	Подпись лица, проводившего инструктаж