ПОЛОЖЕНИЕ
Учреждения здравоохранения
«Брестский областной диспансер спортивной медицины»
«в отношении обработки
персональных данных»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение об обработке и защите персональных данных (далее - Положение) определяет порядок осуществления учреждением здравоохранения «Брестский областной диспансер спортивной медицины» (далее - Учреждение) обработки персональных данных, порядок обработки Учреждением персональных данных лиц, включая порядок сбора, хранения, использования, передачи и защиты таких данных.
2. Упорядочение обращения обработки с персональными данными имеет целью обеспечить права и свободы граждан при обработке персональных данных, сохранение конфиденциальности персональных данных и их защиту.
3. Положение и изменения к нему утверждаются главным врачом Учреждения. Положение является локальным правовым актом Учреждения, обязательным для соблюдения и исполнения работниками, а также иными лицами, участвующими в обработке персональных данных в соответствии с настоящим Положением.
4. Положение разработано на основе и во исполнение:
- Конституции Республики Беларусь;
- Трудового кодекса Республики Беларусь;
- Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981;
- Хартии Европейского союза об основных правах от 12.12.2007;
- Закона Республики Беларусь от 07.05.2021 г. № 99-З «О защите персональных данных»;
-Закона Республики Беларусь от 21.07.2008 г. № 418-З «О регистре населения»
- Закона Республики Беларусь от 10.11.2008 г. № 455-З «Об информации информатизации и защите информации»;
5. Под персональными данными понимается любая информация относящаяся к идентифицированному физическому лицу или физическом лицу, которое может быть идентифицировано.
6. Требование обеспечения конфиденциальности при обработке персональны данных означает обязательное для соблюдения должностными лицами Учреждения, 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.
7. 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 е согласия или распространенные в соответствии с требованиям законодательных актов).
8. Перечни персональных данных и ответственных за хранение и обработ персональных данных утверждается приказом главного врача Учрежден

Обработка и хранение конфиденциальных данных лицами, не указанными в приказе, запрещается.

9. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных Учреждение предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

- знакомит работника под подпись с требованиями Политики оператора в отношении обработки персональных данных Учреждения, с Положением об обработке персональных данных Учреждения, с должностной инструкцией и иными локальными правовыми актами Учреждения в сфере защиты 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.

10. Должностным лицам Учреждения, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа файлы черновиков и вариантов документа переносятся подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных (при необходимости).

11. Согласовывать с руководителем структурного подразделения все вопросы формирования и хранения баз персональных данных (картотек, файловых архивов и др.).

12. Должностные лица Учреждения, работающие с персональными данными, обязаны использовать персональные данные исключительно для целей, связанных с исполнением своих должностных обязанностей.

13. При прекращении выполнения должностной функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), данный работник должен прекратить обработку и передать непосредственному руководителю, и ограничить доступ ко всей персональной обработанной информации.

14. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством Республики Беларусь, Политикой оператора в отношении обработке персональных данных в Учреждении, Положением об обработке и защите персональных данных Учреждения, должностной инструкцией и иными локальными правовыми актами Учреждения в сфере защиты персональных данных. Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом Учреждения на основании письменного или устного поручения руководителя структурного подразделения.

15. Передача сведений и документов третьим лицам, содержащих персональные данные, оформляется путем составления акта по передаче персональных данных с получением письменного согласия на передачу персональных данных с указанием цели передачи персональных данных и указанием сроков.

16. Запрещается передача персональных данных по телефону, факсу, электронной почте, за исключением случаев, установленных законодательством и действующими в Учреждении локальными правовыми актами. 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.

17. Должностные лица Учреждения, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и инженеру 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, удостоверений, пропусков, 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.

18. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Республики Беларусь.

19. Отсутствие контроля со стороны Учреждения за надлежащим исполнением работниками своих обязанностей в области защиты персональных данных не освобождает работников от обязанностей и предусмотренной законодательством Республики Беларусь ответственности за незаконное разглашение (распространение) персональных данных.

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

20. 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.

21. 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 к ним несанкционированный 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 смешивание и хранение материальных носителей персональных данных (документов, дисков, дискет, USB, флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

22. 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.

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

24. Уничтожение (обезличивание) персональных данных осуществляется согласно «Положения о порядке удаления (уничтожения) персональных данных в УЗ «Брестский областной диспансер спортивной медицины».

25. 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

26. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в компьютерной сети Учреждения (далее - КСУ).
Безопасность персональных данных при их обработке в КСУ обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в КСУ информационные технологии.
Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Республики Беларусь требованиям, обеспечивающим защиту информации, и в установленном порядке проходят процедуру оценки соответствия.
27. Допуск лиц к обработке персональных данных осуществляется согласно «Положения о порядке допуска работников и иных лиц к обработке персональных данных в УЗ «Брестский областной диспансер спортивной медицины».
28. Работа с персональными данными в КСУ должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.
29. Доступ к некоторым программам (электронным папкам), в которых содержатся файлы со специальными персональными данными, для ряда должностных лиц ограничен паролем (Программа 1С).
30.Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.
31.При обработке персональных данных в КСУ 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, а также удаления, инсталляции или настройки программного обеспечения.
32. При обработке персональных данных в КСУ разработчиками и администраторами информационных систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в КСУ, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в КСУ, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

33. Специфические требования по защите персональных данных в отдельных автоматизированных системах Учреждения 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

34. Все находящиеся на хранении и в обращении в Учреждении съемные носители (диски, дискеты, USB флеш-накопители, и пр.), содержащие персональные данные, подлежат учету. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку (бирку), на которой указывается его идентификационный учетный номер.

35. Учет и выдачу съемных носителей персональных данных осуществляет инженер. Работники Учреждения получают учтенный съемный носитель от инженера для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале персонального учета съемных носителей персональных данных (далее - журнал учета), который ведется в хозяйственной службе. По окончании работ пользователь сдает съемный носитель для хранения в хозяйственную службу, о чем делается запись в журнале учета.

36. 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, в гостиницах и т. д.

37. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Вынос съемных носителей для непосредственной передачи адресату осуществляется только с письменного разрешения главного врача Учреждения.

38. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено главному врачу и инженеру Учреждения. На утраченные носители составляется акт, отметки об утрате вносятся в журнал персонального учета съемных носителей.

Инженер В.И.Казаренко