УТВЕРЖДЕНО

Приказ главного врача учреждения здравоохранения «26-я городская поликлиника»

от 05.07.2024 № 117

ПОЛОЖЕНИЕ

о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение устанавливает применяемые в учреждении здравоохранения «26-я городская поликлиника» (далее – УЗ «26-я ГП», Оператор) 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 частности через фамилию, имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности, другая информация, необходимая УЗ «26-я ГП» в связи с трудовыми отношениями, а также выполнением функций, полномочий и обязанностей, возложенных на УЗ «26-я ГП» законодательством Республики Беларусь.

3. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения должностными лицами УЗ «26-я ГП», допущенными к обработке персональных данных, иными получившими доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или без 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).

ГЛАВА 2

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ

5. Объем и содержание персональных данных, перечень должностей работников, имеющих доступ к персональным данным, обрабатываемых учреждением, утверждается приказом главного врача УЗ «26-я ГП».

Обработка персональных данных лицами не указанными в приказе, запрещается.

6.  В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных УЗ «26-я ГП» предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

знакомит работника с законом Республики Беларусь от 07.05.2021г. №99-3 «О защите персональных данных», требованиями Политики Оператора в отношении обработки персональных данных УЗ «26-я ГП», с Положением об обработке и защите персональных данных УЗ «26-я ГП», Инструкцией о формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных, информации, составляющей врачебную тайну, отказа от их внесения и обработки и порядке информирования о праве на отказ от внесения информации, составляющей врачебную тайну, в централизованную информационную систему здравоохранения, настоящим Положением о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные, с должностной инструкцией и иными локальными правовыми актами УЗ «26-я ГП» 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. Должностным лицам УЗ «26-я ГП», работающим с персональными данными, запрещается сообщать их устно или письменно (в любой форме) кому бы то ни было, если это не вызвано служебной необходимостью.

8. Должностные лица УЗ «26-я ГП», работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с исполнением своих трудовых обязанностей.

9. При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, электронные 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, и локальными правовыми актами УЗ «26-я ГП» в сфере обеспечения конфиденциальности и безопасности персональных данных.

Передача персональных данных осуществляется должностным лицом УЗ «26-я ГП» только на основании письменного поручения главного врача (исполняющего обязанности главного врача).

11. 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.

12. Должностные лица УЗ «26-я ГП», 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.

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

.

ГЛАВА 3

ОБЯЗАННОСТИ РАБОТНИКОВ ПРИ РАБОТЕ

С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

15. Работники, которые обрабатывают документы и информацию с персональными данными обязаны:

в нерабочее время отключать доступ к рабочему столу через VPN, а также при кратковременном отсутствии на рабочем месте блокировать устройство (компьютер, ноутбук, планшет), которое является собственностью нанимателя;

немедленно информировать руководителя структурного подразделения о фактах утраты (недостачи) документов (отдельных листов), содержащих персональные данные работников, а также при пересылке курьерскими службами или почтой;

 незамедлительно сообщить о попытке или факте взлома устройства;

 вовремя обновлять пароли и программное обеспечение, по требованию системы;

 устанавливать пароли повышенного уровня сложности или использовать двойную аутентификацию;

 для обмена конфиденциальной информацией между работниками использовать только корпоративную почту;

 хранить электронную цифровую подпись в месте исключающем доступ посторонних лиц;

 хранить информацию содержащую персональные данные на бумажных носителях, в местах недоступных для посторонних лиц.

 Работникам запрещено:

 разглашать свои индивидуальные пароли доступа к компьютерным, сетевым и иным информационным ресурсам;

 использовать для сохранения персональных данных работников личные (не принадлежащие Нанимателю) компьютеры (в том числе мобильные — ноутбуки, смартфоны, мобильные телефоны) и съемные USB-накопители, а также подключать их к принадлежащему Нанимателю оборудованию с иной целью ;

отправлять рабочие файлы (сканы, фотографии) на личную электронную почту и другие внешние адреса, в том числе с помощью мессенджеров;

использовать удаленный доступ к рабочему столу или компьютеру, ноутбуку, планшету, смартфону принадлежащих Нанимателю в личных целях;

устанавливать сторонние программы на устройство, которое находится в собственности Нанимателя, без согласования с ним;

использовать Облачные хранилища в целях копирования рабочий конфиденциальной информации;

отключать или заменять Антивирусную защиту на устройстве, которое находится в собственности Нанимателя;

отвечать на запросы, которые требуют предоставления персональных данных работников без согласования с Нанимателем;

допускать к удаленному рабочему столу или устройству, которое находится в собственности нанимателя третьих лиц;

 передавать личную электронную подпись третьим лицам.