Государственное бюджетное профессиональное образовательное учреждение Псковской области «Псковский медицинский колледж»

ГБПОУ ПО "Псковский медицинский колледж"

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ПСКОВСКОЙ ОБЛАСТИ "ПСКОВСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ" 2025.11.12 16:02:37 +03'00'

«УТВЕРЖДАЮ»

Директор ГБПОУ ПО «ПМК»

_____ Г.Е.Егорова

«12» ___X___ 2023 г.

ПРАВИЛА

ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В ГБПОУ ПО «ПМК»

Псков

2023

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила разработаны в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27.07.2006г. No152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17.11.2007г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением другими нормативными правовыми актами Российской Федерации, локальными актами Государственного бюджетного профессионального образовательного учреждения Псковской области «Псковский медицинский колледж» (далее ГБПОУ ПО «ПМК»).

1.2. Правила устанавливают порядок работы с документами, содержащими персональные данные, в целях:

- предотвращения неконтролируемого распространения информации, содержащей персональные данные, в результате ее разглашения должностным лицом, имеющим доступ к информации, содержащей персональные данные, или получения несанкционированного доступа к такой информации;
- предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации, содержащей персональные данные;
- предотвращения утраты, несанкционированного уничтожения или сбоев в процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные.

2.ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. При обработке персональных данных без использования средств автоматизации материальные носители с персональными данными должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах.

2.2. Формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные, осуществляется по согласованию с руководителем структурного подразделения.

2.3. Передача персональных данных не допускается с использованием средств телекоммуникационных каналов связи

(телефон, телефакс, электронная почта и т.п.) без письменного согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации.
2.4. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальную информацию, за исключением данных, содержащихся в запросах или опубликованных в общедоступных источниках.
2.5. При использовании типовых форм документов, характер информации которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:
2.5.1. типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, имя, отчество, фамилию и адрес субъекта персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание способов обработки.
2.5.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации.
2.5.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными не нарушая прав и законных интересов иных субъектов персональных данных.
2.5.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.
2.6. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
2.7. Уничтожение или обезличивание части персональных данных может производиться способом, исключающим дальнейшую обработку этих персональных данных, но с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
2.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями

материального носителя путем изготовления нового материального носителя с уточненными персональными данными.

3. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

3. 1. Безопасность персональных данных при их обработке в автоматизированных информационных системах обеспечивается с помощью организационных мер, средств защиты информации, информационных технологий.

3. 2. Размещение автоматизированных информационных систем, специальное оборудование и сам процесс работы с персональными данными должны исключать возможность неконтролируемого пребывания в соответствующих помещениях посторонних лиц.

3. 3. Компьютеры, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа. Работа на компьютерах с персональными данными без паролей доступа или под чужими (а равно под общими) паролями, не допускается.

3. 4. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе в сети Интернет, не допускается.

3. 5. Технические и программные средства должны соответствовать требованиям законодательства Российской Федерации.

3. 6. При обработке персональных данных в информационной системе должно быть обеспечено:

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

3.6.2. постоянное использование антивирусного, обеспечения и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

4. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИХ ТВЕРДЫМИ КОПИЯМИ), А ТАКЖЕ ИХ УТИЛИЗАЦИИ

4. 1. Не допускается:

4.1.1 хранение съемных носителей с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;
4.1.2. вынос съемных носителей с персональными данными из служебных помещений для работы с ними на дому, в гостиницах, и т.д.
4.2. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.
4.6.3 Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссионно, с составлением соответствующего акта.