Приложение 1
к Приказу от 07.06.2023г. №71

ПОЛОЖЕНИЕ
о защите персональных данных работников и воспитанников Государственного бюджетного учреждения здравоохранения Республики Крым Республиканский специализированный дом ребёнка для детей с поражением центральной нервной системы и нарушением психики «Ёлочка»

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников и воспитанников Государственного бюджетного учреждения здравоохранения Республики Крым Республиканский специализированный дом ребёнка для детей с поражением центральной нервной системы и нарушением психики «Ёлочка» (далее – Учреждение) от несанкционированного доступа, неправомерного их использования или утраты, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Настоящее положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом № 152-ФЗ от 27.07.2006 «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», Устава Учреждения, других нормативных актов в сфере защиты персональных данных и регламентирует порядок работы с персональными данными работников и воспитанников Учреждения.

1.3. Персональные данные относятся к категории конфиденциальной информации.

1.4. Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами.

1.5. В настоящем Положении используются следующие основные понятия:

1) персональные данные и их состав - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая

законодательными и нормативными правовыми актами Российской Федерации, нормативными и распорядительными документами Министерством здравоохранения РК, перечнем персональных данных, обрабатываемых в Учреждении, с указанием целей, оснований, способов и сроков их обработки и локальными актами. К персональным данным могут относиться общедоступные, специальные категории, категории обрабатываемые в информационных системах персональных данных, биометрические и другие. Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, сведения о профессии и иные. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

– субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья субъекта персональных данных и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

– обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия. Категории персональных данных, которые обрабатываются в информационных системах персональных данных:

Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных. Категория 4 – обезличенные и (или) общедоступные персональные данные.

2) лицо, уполномоченное на получение, обработку, хранение, передачу и другое использование персональных данных – работник, организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели и содержание обработки персональных данных;

3) субъект персональных данных – работник, воспитанник и (или) иное лицо, к которому относятся соответствующие персональные данные;

4) работник – физическое лицо, вступившее в трудовые отношения с университетом;

5) воспитанник – несовершеннолетний ребенок, зачисленный в Учреждение;

6) иное лицо – физическое лицо (заказчик, потребитель, исполнитель, арендатор, подрядчик и др.), состоящее в договорных и иных гражданско-правовых отношениях с Учреждением, родитель (опекун, попечитель) воспитанника;

7) обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

8) сбор персональных данных – накопление информации на материальных носителях и (или) в автоматизированных информационных системах;

9) накопление и систематизация персональных данных – организация размещения персональных данных, которое обеспечивает быстрый поиск и отбор нужных сведений, методическое обновление данных, защиту их от искажений, потери;

10) хранение персональных данных – комплекс мероприятий, направленный на обеспечение сохранности полноты и целостности сформированных массивов персональных данных, создание и поддержание надлежащих условий для их использования, а также предупреждение несанкционированного доступа, распространения и использования;

11) уточнение персональных данных – процесс поддержания персональных данных в актуальном состоянии;

12) распространение персональных данных– действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-

телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

13) использование персональных данных – действия (операции) с персональными данными, совершаемые лицом, уполномоченным на получение, обработку, хранение, передачу и другое использование персональных данных в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

14) блокирование персональных данных– временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

15) уничтожение персональных данных– действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

16) обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

17) материальный носитель – бумажный и машиночитаемый носители информации (в том числе магнитный и электронный), на которых осуществляются запись и хранение сведений, на основе которых можно установить личность физического лица;

18) доступ к персональным данным – возможность получения персональных данных и их использования;

19) информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

20) конфиденциальность персональных данных– обязательное для соблюдения лицом, уполномоченным на получение, обработку, хранение, передачу и другое использование персональных данных или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

21) согласие субъекта персональных данных – свободно данное конкретное и сознательное указание о своей воле, которым субъект персональных данных оповещает о своем согласии на обработку касающихся его персональных данных;

22) запрос – изложенное в письменной или устной форме обращение субъекта персональных данных или его законного представителя;

23) письменное обращение – изложенное в письменной форме заявление, направленное по почте либо переданное субъектом персональных данных лично или через его законного представителя;

24) устное обращение – изложенное в устной форме заявление субъекта персональных данных или его законного представителя во время личного приема;

25) третья сторона – любое физическое или юридическое лицо, орган государственной власти или местного самоуправления, кроме субъекта персональных данных, университета (оператора) и лиц, уполномоченных на получение, обработку, хранение, передачу и другое использование персональных данных на законных основаниях;

26) защита персональных данных–технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе деятельности университета;

27) технические средства, позволяющие осуществлять обработку персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

28) несанкционированный доступ – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

29) архивные документы – документы, хранящиеся в архиве, музее и библиотеке университета.

2. Понятие и состав персональных данных

2.1. Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. Любая информация, прямо или косвенно относящаяся к определенному физическому лицу (субъекту персональных данных) относится к его персональным данным (ч. 1 ст. 3 Закона № 152-ФЗ).

В состав персональных данных работника Учреждения входят:

– фамилия, имя, отчество (в том числе предыдущие фамилии имена и (или) отчества, в случаях их изменения);

– пол;

– сведения о гражданстве (подданстве);

– год, месяц, дата и место рождения;

– адрес регистрации и фактического проживания;

– паспортные данные; семейное, социальное положение;

– номер телефона (рабочий, домашний, мобильный) и адрес электронной почты;

– сведения об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование: наименование, номер и дата выдачи, специальность);

– сведения о занимаемой должности, категории персонала;

– дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

– сведения о статусе налогоплательщика;

– сведения о льготах;

– сведения о заработной плате;

– подлинники и копии приказов по личному составу;

– сведения о совместительстве, совмещении;

– доходы, полученные субъектом персональных данных в данном учреждении;

– сведения о платежных реквизитах (номер счета в банковском учреждении, почтовое отделение, номер пластиковой карты);

– сведения о трудовой деятельности и стаже (место работы, должность, общий стаж, страховой, календарный, оплачиваемый),

– данные о состоянии здоровья и группе инвалидности;

– семейное положение, состав семьи (муж/жена/дети) и сведения о близких родственниках;

– место работы или учебы членов семьи и родственников;

– сведения о наличии либо отсутствии судимости;

– сведения о воинском учете и реквизиты документов воинского учета;

– данные об изображении лица, фотография, видео;

– реквизиты страхового свидетельства государственного пенсионного страхования;

– идентификационный номер налогоплательщика;

– сведения о прежнем месте работы;

– иные персональные данные, необходимые для достижения целей деятельности Учреждения, предусмотренных его Уставом.

Под информацией о воспитанниках и их родителей (законных представителей) понимаются сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

В состав персональных данных воспитанников Учреждения входят:

– анкетные и биографические данные;
– сведения о родителях (попечителях), опекунах;
– данные свидетельства о рождении;
– сведения о ближайших родственниках (братья, сестры и др.);
– медицинские сведения;
– педагогическая и психологическая диагностика ребёнка;
– личные дела воспитанников;
– Соглашение между органами опеки, родителями и главным врачом Учреждения;
– иные персональные данные воспитанников, необходимые для достижения целей деятельности Учреждения.

2.3. В соответствии с ч. 1 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» к биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

2.4. Персональные данные о работниках Учреждения, о воспитанниках, их родителях (законных представителях) относятся к конфиденциальной информации. Информация о персональных данных воспитанников предоставляется Учреждением только главным врачом Учреждения, родителем (законным представителем) устно, либо путём заполнения различных анкет, опросных листов, которые могут храниться у главного врача, его заместителей по медицинским вопросам, воспитателей на группе, социальных педагогов, в медицинской карте ребёнка, у врачей, социального педагога. Для лиц, получившего доступ к персональным данным, обязательным является требование не допускать распространение данной информации без согласия главного врача Учреждения, родителя (законного представителя), а также при наличии иного законного основания.

3. Обработка персональных данных

3.1. Под обработкой персональных данных понимается получение, обработка, хранение, комбинирование, передача или любое другое использование персональных данных.

3.2. Обработка персональных данных без использования средств автоматизации.

3.2.1. Обработка персональных данных на материальных носителях считается осуществленной без использования средств автоматизации (неавтоматизированной).

3.2.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

3.2.2.1. Не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы.

3.2.2.2. Персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

3.2.2.3. Документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

3.2.2.4. Дела с документами, содержащими персональные данные, должны иметь внутренние описи документов.

3.2.3. При использовании типовых форм или унифицированных форм документов (далее – типовая форма), характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

3.2.3.1. Типовая форма должна содержать наименование Университета, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных.

3.2.3.2. Типовая форма должна предусматривать графу, в которой субъект персональных данных ставит собственноручную подпись, выражая тем самым свое согласие на обработку персональных данных.

3.2.3.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащих в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

3.2.4 Копирование документов, содержащих персональные данные субъекта персональных данных, должно осуществляться в порядке, исключающим возможность нарушения прав и законных интересов иных субъектов персональных данных, то есть копия документа не должна содержать персональные данные, относящиеся к другим субъектам персональных данных.

3.2.5. 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 фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3.2.6. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних носителях информации (флэш-накопитель, компакт-диск и др.).

3.2.7. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

3.2.8. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.3. Обработка персональных данных с использованием средств автоматизации.

3.3.1. Обработка персональных данных, содержащихся в базах данных информационной системы, осуществляется с помощью технических средств.

3.3.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:

– при отсутствии установленных и настроенных сертифицированных средств защиты информации для информационной системы персональных данных, попадающих под эти требования в соответствии с законодательством Российской Федерации;

– при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

3.4. Не допускается отвечать на вопросы, связанные с передачей персональной информации в личной беседе, по телефону или факсу.

3.5. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри Учреждения).

4.1.1. Право доступа к персональным данным субъекта персональных данных имеют:

– главный врач;

– руководители подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения);

– лица, уполномоченные на получение, обработку, хранение, передачу и другое использование персональных данных;

– субъект персональных данных.

4.1.2. В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией главного врача, доступ к персональным данным может быть предоставлен иному работнику, который не назначен лицом, уполномоченным на получение, обработку, хранение, передачу и другое использование персональных данных, который также подписывает соглашение (обязательство) о неразглашении конфиденциальной информации (персональных данных).

4.1.3. Доступ субъекта персональных данных к своим персональных данным предоставляется при личном обращении к лицу, уполномоченному на получение, обработку, хранение, передачу и другое использование персональных данных или через законного представителя, а также путем

направления им запроса. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. При личном обращении субъект персональных данных или его законный представитель должен предъявить документ, удостоверяющий его личность, на основании которого лицо, уполномоченное на получение, обработку, хранение и передачу персональных данных, произведет идентификацию личности субъекта или его законного представителя.

4.2. Внешний доступ.

– военные комиссариаты;

– правоохранительные органы (суды общей юрисдикции, арбитражные суды, Конституционный суд, органы прокуратуры РФ, Следственный комитет РФ, Федеральная миграционная служба, Федеральная служба безопасности, Федеральная таможенная служба, Федеральная служба судебных приставов, органы внутренних дел);

– профессиональные союзы и иные органы.

8.2.2 Организации, в которые субъект персональных данных может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения и т.п.), могут получать доступ к персональным данным работника, воспитанника только в случае его письменного разрешения.

8.2.3 Сведения об уже уволенном работнике могут быть предоставлены сторонним организациям только на основании письменного запроса на официальном бланке организации, с приложением копии заявления работника. Аналогичное правило применяется в отношении выбывших из Учреждения воспитанников.

8.2.4 Родственники и члены семей. Персональные данные субъекта персональных данных могут быть предоставлены родственникам или членам его семьи только с письменного согласия самого субъекта персональных данных.

5. Защита персональных данных

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные

обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

5.4. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральными законами.

5.5. Внутренняя защита.

5.5.1. В целях обеспечения сохранности и конфиденциальности персональных данных субъектов персональных данных все операции по сбору, накоплению, систематизации и хранению данной информации должны выполняться только лицами, уполномоченными на получение, обработку, хранение, передачу и другое использование персональных данных. Все лица, уполномоченные на получение, обработку, хранение, передачу и другое использование персональных данных, обязаны подписать соглашение (обязательство) о неразглашении конфиденциальной информации (персональных данных), не содержащей сведений, составляющих государственную тайну.

5.5.2. Ответы на запросы (письменные обращения) юридических лиц в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке университета и в том объеме, который позволяет не разглашать излишний объем персональных данных о субъектах персональных данных. Если же юридическое лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъектов персональных данных, либо отсутствует письменное согласие субъекта персональных данных на предоставление его персональных данных, лицо, уполномоченные на получение, обработку, хранение, передачу и другое использование персональных данных обязано отказать в предоставлении персональных данных юридическому лицу.

5.5.3. Электронно-вычислительные машины, средствами которых осуществляется работа с персональными данными, должны иметь парольную систему доступа.

5.4. Внешняя защита.

5.4.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

5.4.2. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в структурных подразделениях, уполномоченных на обработку персональных данных.

5.4.3. Для обеспечения внешней защиты персональных данных необходимо разрабатывать и соблюдать организационные меры и использовать технические средства и системы в соответствии законодательством Российской Федерации.

5.6. Внешняя защита.

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности образовательного учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

5.6.3. Для обеспечения внешней защиты персональных данных работников и воспитанников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников и воспитанников.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников и воспитанников.

6. Права и обязанности субъекта

6.1. Закрепление прав субъекта, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных;

- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

- определять своих представителей для защиты своих персональных данных;

- на сохранение и защиту своей личной и семейной тайны.

6.3. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.

- своевременно сообщать работодателю об изменении своих персональных данных.

6.4. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.5. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Главный врач, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную,

административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским кодексом РФ лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

8. Заключительные положения

8.1. Настоящее Положение утверждается и вводится в действие приказом главного врача Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников и воспитанников.

8.2. В данное Положение могут вноситься изменения и дополнения, которые утверждаются приказом главного врача Учреждения.