|  |  |
| --- | --- |
|  | УТВЕРЖДЕНОПриказом и.о.главного врача ГБУЗРК «Детский санаторий «Кедр» от 20.04.2016г. № 78-ОД |

**Положение о защите**

**персональных данных работников ГБУЗРК «Детский санаторий «Кедр»**

1. **Общие положения**
	1. Настоящим Положением определяется порядок обращения с персональными данными работников Государственного бюджетного учреждения здравоохранения Республики Коми «Детский санаторий «Кедр» (далее Санаторий).
	2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Санатория и её работников в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.
	3. Персональные данные работника – любая информация, относящаяся к конкретному работнику (субъекту персональных данных) и необходимая работодателю в связи с трудовыми отношениями.
	4. Настоящее Положение разработано на основании ст.24 Конституции Российской Федерации, гл. 14 Трудового Кодекса Российской Федерации, Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информатизации и защите информации», Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных».
	5. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.
	6. Должностные лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие её, несут ответственность в соответствии с законодательством Российской Федерации за нарушение обработки и порядка использования этой информации.
	7. Настоящее Положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным сотрудников санатория.
	8. Все работники Санатория должны быть ознакомлены с настоящим Положением под роспись.
2. **Понятие и состав персональных данных**
	1. Для целей настоящего Положения используются следующие основные понятия:
* **персональные данные** – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
* **обработка персональных данных работника** – любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
* **распространение персональных данных** – действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц;
* **предоставление персональных данных** – действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц;
* **блокирование персональных данных** – временное прекращение обработки персональных данных работников (за исключение случаев, если обработка необходима для уточнения персональных данных);
* **уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников;
* **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику;
* **информация** – сведения (сообщения, данные) независимо от формы их представления;
* **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или её материальный носитель.
	1. Состав персональных данных работника:
* анкетные и биографические данные;
* данные документа удостоверяющего личность (серия, номер паспорта, кем и когда выдан);
* дата и место рождения;
* адрес регистрации и адрес фактического проживания;
* индивидуальный номер налогоплательщика (ИНН);
* номер страхового свидетельства (СНИЛС);
* реквизиты полиса медицинского страхования;
* сведения о наличии или отсутствии судимости;
* домашний и сотовый телефон;
* сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи);
* форма профессионального послевузовского образования;
* данные об аттестации работника;
* данные о профессиональной переподготовке или повышении квалификации;
* сведения об ученной степени;
* сведения о государственных наградах, знаках отличия;
* сведения о трудовой деятельности (стаж, места работы, должности, периоды работы, причины увольнения, сведения о трудовой книжке (№, серия, дата выдачи, записи в ней), сведения о командировках, отпусках, поощрениях, данные о трудовом договоре (№, дата, условия, гарантии)).
* сведения о проведении служебных проверок, дисциплинарных расследований;
* сведения о стаже;
* номер расчетного счета, номер банковской карты;
* сведения о доходах, об имуществе и обязательствах имущественного характера, в т.ч. членов семьи, а также о расходах;
* тип и сумма налогового вычета;
* сведения об инвалидности, временной нетрудоспособности и прохождении диспансеризации;
* сведения о составе семьи и сведения о близких родственниках;
* реквизиты свидетельств о государственной регистрации актов гражданского состояния;
* сведения о семейном положении;
* сведения о воинском учете и реквизиты документов воинского учета;
* сведения о социальных льготах;
* информация о владении иностранными языками (степень владения);
* сведения о гражданстве.

Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения – соответствующий гриф ограничения на них не ставится.

1. **Обязанности работодателя**
	1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:
		1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
		2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.
		3. Все персональные данные работника следует получать у него самого. Если персональные данные работника, возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
		4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.
		5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
		6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.
		7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.
2. **Обязанности работника**
	1. Передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации.
	2. Своевременно сообщать работодателю об изменениях своих персональных данных.
3. **Права работника**
	1. Требовать исключения или исправления неверных или неполных персональных данных.
	2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные.
	3. На сохранение и защиту своей личной и семейной тайны.
4. **Сбор, обработка и хранение персональных данных**
	1. Порядок получения персональных данных:
		1. Все персональные данные работника следует получать у него самого. Если персональные данные работника, возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
		2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.
		3. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
	2. При передаче персональных данных работника работодатель должен соблюдать следующие требования:
* не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных федеральным законом;
* не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
* предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
* разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
* не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
* передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.
	1. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
	2. При передаче персональных данных работника потребителям за пределы учреждения работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.
	3. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
	4. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
	5. По возможности персональные данные обезличиваются.
1. **Доступ к персональным данным сотрудника**
	1. Внутренний доступ (доступ внутри организации).

Право доступа к персональным данным сотрудника имеют:

* главный врач санатория;
* начальники структурных подразделений по направлению деятельности;
* специалист по кадрам;
* работники бухгалтерии;
* экономист;
* специалист по охране труда;
* сам работник, носитель данных.

Другие сотрудники организации имеют доступ к персональным данным работника только с письменного согласия самого работника, носителя данных.

* 1. Внешний доступ.
		1. К числу массовых потребителей персональных данных вне учреждения можно отнести государственные и негосударственные функциональные структуры:
* налоговые инспекции;
* правоохранительные органы;
* органы статистики;
* военкоматы;
* органы социального страхования;
* пенсионные фонды
* и т.д.
	+ 1. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
		2. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.
		3. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии заверенного заявления работника.

* + 1. Родственники и члены семей.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия.

1. **Защита персональных данных**

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.

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.

Защита персональных данные 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 учреждения.

* 1. «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами учреждения. Для защиты персональных данных работников необходимо соблюдать ряд мер:

* ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
* строгое избирательное и обоснованное распределение документов и информации между работниками;
* рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
* знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
* наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
* определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
* организация порядка уничтожения информации;
* воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
* не допускается выдача личных дел сотрудников на рабочие места. Личные дела могут выдаваться на рабочее место только руководителю учреждения, в исключительных случаях, по письменному разрешению руководителя учреждения, руководителю структурного подразделения.
	+ 1. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем.

* 1. «Внешняя защита»

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.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

* + 1. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:
* порядок приема, учета и контроля деятельности посетителей;
* пропускной режим учреждения;
* технические средства охраны, сигнализации;
* порядок охраны территории, зданий, помещений, транспортных средств;
* требования к защите информации при интервьюировании и собеседованиях.
	+ 1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
		2. Все лица, связанные с получением, обработкой и защитой персональных данных сотрудника обязаны заключить «Соглашение о неразглашении персональных данных сотрудников учреждения».
1. **Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника**

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.