

Государственное бюджетное учреждение Республики Крым
«Солено-Озерский специальный дом-интернат для престарелых и инвалидов»

ПОЛОЖЕНИЕ
о конфиденциальной информации

1. Термины и определения

Для целей настоящего Положения используются следующие термины и определения.

Конфиденциальная информация – любые сведения, составляющие служебную, коммерческую тайну, включая персональные данные работников и получателей социальных услуг (далее-ПСУ).

Обладатель конфиденциальной информации – лицо, которое владеет информацией, составляющей конфиденциальную информацию, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации. Обладателем информации, составляющей конфиденциальную информацию, является Государственное бюджетное учреждение Республики Крым «Солено-Озерский специальный дом-интернат для престарелых и инвалидов» (далее- Учреждение).

Информация – сведения (сообщения, данные) независимо от формы их представления.

Служебная тайна – финансово-экономическая или иная информация, которая имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой обладателем такой информации введен режим конфиденциальности. Информация может быть отнесена к служебной тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений и не влечет (не может повлечь) получения прибыли обладателем такой информации. Служебную тайну Учреждения составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электронной и почтовой связи, которые стали известны работнику Учреждения в связи с исполнением им возложенных на него трудовых обязанностей. К служебной тайне не относится информация, разглашенная Учреждением самостоятельно или с его согласия, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством РФ.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Информация может быть отнесена к коммерческой тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений, либо в результате гражданско-правовых отношений, влекущая или могущая повлечь получение прибыли обладателем такой информации.

Врачебная тайна – информация о состоянии здоровья работников и ПСУ, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении.

Персональные данные работника, ПСУ – любая информация, относящаяся к работнику, ПСУ как субъекту персональных данных, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, сведения о фактах, событиях и обстоятельствах жизни работника, ПСУ, позволяющие идентифицировать его личность.

Доступ к конфиденциальной информации – ознакомление определенных лиц с информацией, составляющей тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача конфиденциальной информации – передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление информации, составляющей тайну, - передача информации, составляющей тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение конфиденциальной информации – действие или бездействие, в результате которых информация, составляющая тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия

обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

2. Общие положения

2.1. Директор осуществляет общее управление обеспечением режима безопасности сведений, содержащих конфиденциальную информацию.

2.2. Лица, допущенные к конфиденциальной информации, должны быть ознакомлены с настоящим Положением под подпись.

2.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не предусмотрено законодательством РФ.

2.4. Настоящее Положение утверждается и вводится в действие приказом директора учреждения и является обязательным для исполнения всеми работниками учреждения, имеющими доступ к конфиденциальной информации учреждения.

2.5. Работники учреждения должны быть ознакомлены под подпись с документами учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3. Информация, являющаяся конфиденциальной, и доступ к ней

3.1. Перечень конфиденциальной информации учреждения определяется настоящим Положением.

3.2. Каждый работник, получающий доступ к конфиденциальной информации, в том числе к персональным данным, подписывает обязательство о неразглашении конфиденциальной информации, в том числе сведений о персональных данных, а также уведомление об ответственности в случае нарушения требований действующего законодательства в сфере обработки персональных данных.

3.3. Список работников, допущенных к работе с конфиденциальной информацией, утверждается приказом директора.

3.4. Состав персональных данных определяется в соответствии с приложением 1 к Правилам обработки персональных данных в ГБУ РК «Солено-Озерский СДИПИ».

4. Порядок обращения конфиденциальной информации

4.1. Сведения, составляющие конфиденциальную информацию могут быть выражены в письменной, устной и иных формах. Конфиденциальная информация, ставшая известной работнику из письменных, устных и иных источников, охраняется равным образом.

4.2. Конфиденциальная информация, ставшая известной работнику из устных источников, не должна быть им разглашена. В случае разглашения данной информации работник несёт ответственность в установленном законодательством порядке.

4.3. Письменные и машинные источники информации, содержащие служебную и коммерческую тайну, подлежат учёту и специальному обозначению.

4.4. В случае необходимости оперативного доведения до заинтересованных лиц сведений, составляющих тайну, директором ставится резолюция на самом документе, содержащем служебную или коммерческую тайну. Такое разрешение должно содержать перечень фамилий работников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись директора и дату. Директор может при необходимости предусмотреть ограничения в доступе конкретных работников к определенным сведениям.

4.5. Не допускается разглашение сведений, составляющих врачебную тайну лицами, которым они стали известны при исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных в настоящем Положении.

4.6. С согласия гражданина или его законного (уполномоченного) представителя допускается передача сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в интересах обследования и лечения гражданина

4.7. Уполномоченными представителями являются лица, действующие на основании нотариально удостоверенной доверенности.

4.8. Полномочия представителя подтверждаются нотариально удостоверенной доверенностью.

4.9. Под обработкой персональных данных понимается сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных и любое другое использование персональных данных.

4.10. В целях обеспечения прав и свобод человека и гражданина работники учреждения при обработке персональных данных обязаны соблюдать следующие общее требование:

обработка персональных данных может осуществляться исключительно в целях оказания услуг

надлежащего качества и объема, в целях выполнения условий трудового договора, в иных предусмотренных законодательством случаях;

4.11. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

4.12. Персональные данные не могут быть использованы в целях причинения имущественного, физического и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

4.13. Передача персональных данных возможна только с согласия субъекта персональных данных или его законных представителей в случаях, прямо предусмотренных законодательством.

4.14. При передаче персональных данных за пределы учреждения, работники учреждения не должны сообщать эти данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина или в случаях, установленных федеральным законом.

4.15. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (с использованием средств автоматизации и без использования средств автоматизации) носители информации.

4.16. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

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

5. Охрана конфиденциальной информации

5.1. В целях охраны конфиденциальной информации работник обязан:

- 1) соблюдать установленный режим охраны такой информации;
- 2) не разглашать конфиденциальные сведения, ставшие ему известными из письменных, устных и иных источников и не использовать эту информацию в личных целях;
- 3) обеспечить невозможность утраты (целостность и сохранность, соблюдение порядка хранения) документов, содержащих указанные сведения;
- 4) обеспечить невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию, находящимся в его ведении;
- 5) работать только с теми конфиденциальными сведениями и документами, к которым он получил доступ в силу своих служебных обязанностей, знать какие конкретно сведения подлежат защите, а также строго соблюдать правила пользования ими.

5.2. Работники, допущенные к конфиденциальной информации, обязаны незамедлительно сообщить директору учреждения о пропаже документов, машинных носителей информации, содержащих конфиденциальные сведения, а также о несанкционированном доступе лиц к такой информации, или о попытке подобного доступа.

5.3. По факту разглашения конфиденциальной информации, потери документов и иного несанкционированного доступа к конфиденциальным сведениям, проводится служебное расследование, по результатам которого виновные лица привлекаются к ответственности.

5.4. При участии в работе сторонних организаций сотрудник может знакомить их представителей со сведениями, составляющими конфиденциальную информацию, только с письменного разрешения директора. Директор при этом должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть сообщена информация, подлежащая защите.

5.5. По общему правилу доступ посторонних лиц к сведениям, составляющим врачебную тайну, не допускается, за исключением случаев, установленных действующим законодательством, а также настоящим Положением.

5.6. Защита персональных данных представляет собой 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 организации.

5.7. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена в порядке, установленном действующим законодательством.

5.8. Защита включает в себя следующие меры:

- ограничение и регламентация доступа работников к персональным данным с установлением конкретных прав доступа;
- строгое избирательное и обоснованное распределение документов и информации между

работниками учреждения;

- рациональное и эргономичное размещение рабочих мест работников учреждения, имеющих доступ к персональным данным, при котором исключалась бы случайная утечка защищаемой информации;
- ознакомление работников учреждения с требованиями нормативно- методических документов по защите информации о персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации, содержащей персональные данные работников;
- регламентация обращения документов, содержащих персональные данные, на рабочих местах работников учреждения;
- принятие в установленном порядке мер по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства;
- привлечение к дисциплинарной ответственности лиц, виновных в нарушении законодательства о персональных данных.

6. Ответственность за разглашение конфиденциальной информации

6.1. Работник, который в связи с исполнением трудовых обязанностей получил доступ к сведениям, составляющим конфиденциальную информацию, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления, в соответствии со ст. 192 Трудового кодекса (далее ТК РФ) выносятся дисциплинарное взыскание.

6.2. Каждый работник учреждения, получающий для работы конфиденциальный документ (иной материальный носитель конфиденциальной информации), содержащий информацию о персональных данных работников и ПСУ, несет ответственность за сохранность носителя и конфиденциальность информации.

6.3. Работник, осуществляющий сбор сведений, незаконными способами в целях разглашения либо незаконного использования этих сведений, а также за их разглашение или незаконное использование, совершенные из корыстной или иной личной заинтересованности и причинивший крупный ущерб организации, в соответствии со ст. 183 Уголовного кодекса РФ несет уголовную ответственность.

6.4. Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, с учетом причиненного гражданину ущерба несут за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации.

6.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

6.5. 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 наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

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



Принимать и выдавать
судебные акты (судебные)
и
Душевный 0559 ПК
и
Судебный 0559 ПК
и
В. И. Сидоров