

## **ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### **1 Общие положения**

1.1. Настоящее Положение по обработке персональных данных (далее — Положение) Государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» (далее – Учреждение) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» №149 от 27.07.2006г., Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Правилами внутреннего трудового распорядка Учреждения.

1.2. Цель разработки Положения — определение порядка обработки персональных данных сотрудников Учреждения и иных субъектов персональных данных, персональные данные которых подлежат обработке; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника Учреждения, при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения руководителем Учреждения (далее – Руководителем) и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом директором ГБУЗ «ЧОМИАЦ».

1.4. Все работники Учреждения должны быть ознакомлены с настоящим Положением.

## 2 Определения

2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.2. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

2.3. 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;

2.4. 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;

2.5. Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором 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;

2.6. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

2.7. 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;

2.8. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

2.9. 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;

2.10. Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

2.11. Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.12. Информационно-аналитическая система сбора и обработки данных медицинских и фармацевтических работников, состоянии здоровья населения, лекарственного обеспечения Челябинской области – это набор различных информационных систем (в т.ч.: «Российский государственный медико-дозиметрический регистр лиц, подвергшихся воздействию радиации вследствие катастрофы на Чернобыльской АЭС»; «Региональный сегмент Федерального регистра медицинских и фармацевтических работников муниципальных и государственных учреждений здравоохранения Челябинской области»; «Диспансеризация детей декретированных возрастов Челябинской области»; «Выписка рецептов и учет ОНЛС»; «Государственный регистр больных сахарным диабетом»; «Иммунизация населения г. Челябинска и Челябинской области»; «Региональная телемедицинская система челябинской области»; «Федеральный регистр медицинских работников») объединенных в данном документе в рамках осуществления деятельности Государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр».

### **3 Основные понятия и состав персональных данных**

3.1. Состав персональных данных, обрабатываемых в информационных системах персональных данных (далее – ИСПДн) Учреждения, определяется «Перечнем сведений, содержащих персональные данные».

3.2. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в Учреждении при его приеме, переводе и увольнении.

3.2.1. Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника).

3.2.2. При оформлении работника в Учреждение, сотрудником в обязанности которого вменены обязанности по кадровому учету, заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

- сведения о воинском учете;

- данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;

- сведения об аттестации;

- сведения о повышении квалификации;

- сведения о профессиональной переподготовке;

- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;

- сведения о социальных гарантиях;

- сведения о месте жительства и контактных телефонах.

3.2.3. Ответственный за учет кадров создает и хранит следующие группы документов, содержащие персональные данные работников в единичном или сводном виде:

3.2.3.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

3.2.3.2. Организационно-распорядительная документация Учреждения (Положения, должностные инструкции работников, приказы руководителя); документы по планированию, учету, анализу и отчетности в части работы с сотрудниками Учреждения.

3.3. Комплекс документов, сопровождающий процесс работы информационной аналитической системы сбора и обработки данных медицинских и фармацевтических работников, состоянии здоровья населения, лекарственного обеспечения Челябинской области.

В процессе работы информационной аналитической системы сбора и обработки данных медицинских и фармацевтических работников, состоянии здоровья населения, лекарственного обеспечения Челябинской области предоставляются следующие виды документов:

3.3.1.1.Регистры медицинских работников лечебно-профилактических учреждений;

3.3.1.2.Акты экспертизы реестра рецептов лекарственных средств;

3.3.1.3.Выписка из реестра лекарственных средств

3.3.1.4.Карта причин смерти (КПС) лица, подвергшегося воздействию радиации в результате катастрофы на ЧАЭС

3.3.1.5.Регистрационная карта онкологического заболевания лица, подвергшегося воздействию радиации в результате катастрофы на ЧАЭС

3.3.1.6.Выписка из медицинской карты стационарного больного

3.3.1.7.Выписка эпикриз

3.3.1.8.Верификация данных о случаях гемабластозов

3.3.1.9.Результат проверки качества данных региональной базы по гемабластозам

3.3.1.10. Корешок медицинского свидетельства о смерти

3.3.1.11. Протокол патологоанатомического вскрытия

3.3.1.12. Протокол судебно-медицинской экспертизы

3.3.1.13. Копия справки медико-социальной экспертизы

3.3.1.14. Копия свидетельства о рождении

3.3.1.15. Копия свидетельства о смерти

3.3.1.16. Копия паспорта

3.3.1.17. Копия военного билета

В дальнейшем в ИСПДн Учреждения обрабатываются персональные данные согласно Перечню сведений, содержащих персональные данные.

## **4 Сбор, обработка и защита персональных данных**

### **4.1. Порядок получения персональных данных.**

4.1.1. Все персональные данные сотрудников Учреждения и прочих физических лиц следует получать у них самих. Должностное лицо Учреждения должно сообщить о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

4.1.2. Учреждение не имеет права получать и обрабатывать персональные данные сотрудников об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

4.1.3. Учреждение как работодатель вправе обрабатывать персональные данные сотрудников и прочих физических лиц только с их письменного согласия.

4.1.4. Согласие субъекта не требуется в следующих случаях:

4.1.5. обработка персональных данных осуществляется на основании Трудового кодекса РФ или федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

4.1.6. обработка персональных данных осуществляется в целях исполнения трудового договора;

4.1.7. обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4.1.8. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

4.2. Порядок обработки, передачи и хранения персональных данных.

4.2.1. Субъект предоставляет должностному лицу Учреждения достоверные сведения о себе. Должностное лицо проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами.

4.2.2. Руководитель и сотрудники Учреждения (операторы) при обработке персональных данных сотрудника должны соблюдать следующие общие требования:

4.2.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

4.2.2.2. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами.

4.2.2.3. Персональные данные для обработки в информационной аналитической системе сбора и обработки данных, медицинских и фармацевтических работников, состоянии здоровья населения, лекарственного обеспечения Челябинской области в Учреждении, обрабатываются на основании Федерального закона «О персональных данных» № 152-ФЗ, приказов Министерства здравоохранения РФ, приказов Министерства здравоохранения Челябинской области и иных нормативных актов РФ.

4.2.2.4. При принятии решений, затрагивающих интересы субъекта, Учреждение, как оператор, не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4.2.2.5. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением как оператором за счет своих средств в порядке, установленном федеральным законом.

4.2.2.6. Сотрудники и их представители должны быть ознакомлены под подпись с документами Учреждения, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

4.2.2.7. Во всех случаях отказ субъекта от своих прав на сохранение и защиту персональных данных недействителен.



## **5 Передача и хранение персональных данных**

5.1. При передаче персональных данных субъекта Учреждение должно соблюдать следующие требования:

5.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом.

5.1.2. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные субъекта, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

5.1.3. Осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением.

5.1.4. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций и служебных обязанностей.

5.1.5. Передавать персональные данные сотрудников представителям в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

5.1. Хранение и использование персональных данных:

5.1.1. Персональные данные субъектов обрабатываются и хранятся в режимных помещениях ГБУЗ «ЧОМИАЦ» и на учтённых машинных носителях в соответствии с Инструкцией по учёту машинных носителей утверждённой приказом директором ГБУЗ «ЧОМИАЦ».

5.1.2. Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде — в локальной компьютерной сети, в компьютерных программах и электронных базах данных.

5.2. При получении персональных данных не от субъекта (за исключением случаев, если персональные данные были предоставлены Учреждению на основании федерального закона или если персональные данные являются общедоступными), Учреждение до начала обработки таких персональных данных обязано предоставить субъекту следующую информацию:

5.2.1. наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

5.2.2. цель обработки персональных данных и ее правовое основание;

5.2.3. предполагаемые пользователи персональных данных;

5.2.4. установленные Федеральным законом №152 «О персональных данных» права субъекта персональных данных.

## **6 Доступ к персональным данным сотрудников**

6.1. Перечень лиц, имеющих право доступа к персональным данным, определяется приказом о «Списке лиц, доступ которых к персональным данным обрабатываемым в информационных системах ГБУЗ «ЧОМИАЦ» необходим для выполнения служебных обязанностей», утверждённым Руководителем Учреждения.

6.2. Субъект персональных данных, чьи персональные данные обрабатываются в информационной системе Учреждения имеет право:

6.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта.

6.2.2. Требовать от Учреждения уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для оператора персональных данных.

6.2.3. Получать от оператора:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

- перечень обрабатываемых персональных данных и источник их получения;

- сроки обработки персональных данных, в том числе сроки их хранения;

- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

6.2.4. Требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.3. Внешний доступ (другие организации и граждане).

6.3.1. Предоставление сведений о персональных данных работников без соответствующего их согласия возможно в следующих случаях:

6.3.1.1. в целях предупреждения угрозы жизни и здоровья работника;

6.3.1.2. при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;

6.3.1.3. при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов.

6.3.2. Работник, о котором запрашиваются сведения, должен быть уведомлён о передаче его персональных данных третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно: стихийных бедствий, аварий, катастроф.

6.3.3. Запрещается передача персональных данных работника в коммерческих целях без его согласия.

6.4. Передача информации третьей стороне возможна только при письменном согласии субъектов.

## **7 Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

В соответствии со ст. 24 Федерального закона № 152 «О персональных данных» лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

### **7.1. Ответственность работодателя**

В соответствии со ст. 13.11 КоАП РФ нарушение установленного законом порядка сбора, хранения, использования или распространения

информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа:

- на граждан - от 300 до 500 руб.;
- на должностных лиц - от 500 до 1000 руб.;
- на юридических лиц - от 5000 до 10 000 руб.

Работодатель как юридическое лицо может быть привлечен к административной ответственности за нарушение порядка сбора, хранения, использования или распространения персональных данных.

Помимо организации, ответственность за нарушение несет ее руководитель как должностное лицо. Под должностным лицом понимается лицо, выполняющее организационно-распорядительные или административно-хозяйственные функции.

#### 7.2. Ответственность работника, имеющего доступ к персональным данным

Согласно ст. 90 ТК РФ работник, по вине которого было допущено нарушение норм, регулирующих получение, обработку и защиту персональных данных других работников, может быть привлечен к дисциплинарной и материальной, а также к гражданско-правовой, административной и уголовной ответственности.

#### 7.3. Административная ответственность работника, имеющего доступ к персональным данным

На основании ст. ст. 2, 3, 5, 6 Закона о персональных данных персональные данные относятся к информации, доступ к которой ограничен. В соответствии со ст. 13.14 КоАП РФ разглашение подобной информации (за исключением случаев, если такое разглашение влечет уголовную ответственность) лицом, получившим доступ к ней в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа:

- на граждан - от 500 до 1000 руб.;
- на должностных лиц - от 4000 до 5000 руб.

Следовательно, если будет установлено, что разглашение персональных данных произошло по вине работника, ответственного за хранение, обработку и использование персональных данных других работников, то его могут привлечь к административной ответственности в виде штрафа.

#### 7.4. Дисциплинарная ответственность работника, имеющего доступ к персональным данным

Неправомерное разглашение персональных данных лицом, в чьи обязанности входит соблюдение правил хранения, обработки и использования такой информации, также является основанием для привлечения этого лица к дисциплинарной ответственности (ст. 90 ТК РФ). Согласно ст. 192 ТК РФ за совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;
- 3) увольнение по соответствующим основаниям.

#### 7.5. Уголовная ответственность работника, имеющего доступ к персональным данным

Уголовная ответственность за незаконные действия, нарушающие права личности в области защиты персональных данных, установлена в Уголовном кодексе РФ. Так, согласно ст. 137 УК РФ "Нарушение неприкосновенности частной жизни", незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан, наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до одного года, либо арестом на срок до 4х месяцев, либо лишением свободы на срок до 2х лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3х лет.

#### 7.6. Материальная ответственность работника, имеющего доступ к персональным данным

Статьей 90 ТК РФ предусмотрена материальная ответственность за виновное нарушение норм, регулирующих получение, обработку и защиту персональных данных работников. Так, в результате незаконного распространения информации о персональных данных работника последнему может быть причинен моральный вред, подлежащий возмещению работодателем. В соответствии со ст. 238 ТК РФ работник обязан возместить

работодателю причиненный последнему прямой действительный ущерб. Согласно ч. 2 указанной статьи под прямым действительным ущербом также понимается необходимость возмещения ущерба третьим лицам. Следовательно, если вред работнику был допущен по вине лица, которое было ответственно за неразглашение персональных данных, то работодатель может привлечь последнее к материальной ответственности за ущерб, который был нанесен работнику такими действиями. В соответствии с п. 7 ч. 1 ст. 243 ТК РФ материальная ответственность в полном размере причиненного ущерба возлагается на работника в случае разглашения сведений, составляющих охраняемую законом тайну.

7.7. Гражданско-правовая ответственность работника, имеющего доступ к персональным данным

В соответствии со ст. 151 ГК РФ, если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. Согласно ч. 2 ст. 1099 ГК РФ моральный вред, причиненный действиями (бездействием), нарушающими имущественные права гражданина, подлежит компенсации в случаях, предусмотренных законом. На основании ст. 152 ГК РФ гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности. Следовательно, если в результате нарушения норм, регулирующих хранение, обработку и использование персональных данных работника, допущенного лицом, ответственным за осуществление вышеперечисленных действий с персональными данными, работнику причинен имущественный ущерб или моральный вред, то он подлежит возмещению в денежной форме в соответствии со статьями Гражданского кодекса РФ.