

# Политика конфиденциальности

## 1. ОСНОВНЫЕ ПОНЯТИЯ

В настоящей Политике используются следующие основные понятия:

1.1. Субъектами персональных данных ГУЗ ТО «Тульская областная клиническая больница» (далее Учреждение) являются:

- работники Учреждения;
- претенденты на замещение вакантной должности в Учреждении;
- пациенты Учреждения.

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

1.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), 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.

1.4. Конфиденциальность персональных данных – обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным Законом.

## 2. Информация об операторе.

Наименование: Государственное учреждение здравоохранения Тульской области «Тульская областная клиническая больница».

Адрес местонахождения: 300053, Российская Федерация, г. Тула, ул. Яблочкова д.1-А.

Почтовый адрес: 300053, Российская Федерация, г. Тула, ул. Яблочкова д.1-А.

Тел. :+7(4872) 48-65-04

ИНН : 7105008306

E-mail: [Guz.tokb2@tularegion.ru](mailto:Guz.tokb2@tularegion.ru)

## 3. Принципы и цели обработки персональных данных.

3.1. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

3.1.1. Учреждение в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона 152-ФЗ «О персональных данных»;

3.1.2. Учреждение ограничивается достижением конкретных, заранее определённых и законных целей;

3.1.3. Обработке подлежат только персональные данные, которые отвечают целям их обработки;

3.1.4. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

3.1.5. Учреждение не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность);

3.1.6. Учреждение не производит трансграничную (на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных;

3.2. Учреждение обрабатывает персональные данные пациента исключительно в следующих целях:

3.2.1 Обработка сведений, необходимых для реализации полномочий учреждения, оказание услуг в сфере здравоохранения и предоставления квалифицированной медицинской помощи.

3.3. Учреждение обрабатывает персональные данные работника и соискателя исключительно в следующих целях:

3.3.1. Принятие решения о трудоустройстве соискателя;

3.3.2. Заключение и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера, содействие в обучении и продвижении по службе, контроля количества и качества выполняемой работы, расчет и перечисление заработной платы, удержание из заработной платы.

#### **4. Меры по обеспечению безопасности персональных данных при их обработке.**

4.1. Учреждение при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них, а именно:

Назначение приказом руководителя Учреждения №242 от 28.04.2017 «О назначении ответственного лица за организацию обработки персональных данных в ГУЗ ТО «Тульская областная клиническая больница»» ответственного лица за организацию обработки персональных данных, руководство выполнением работ по комплексной защите информации в учреждении, обеспечение эффективного применения имеющихся организационных и инженерно-технических мер по защите информации, обеспечение контроля за выполнением требований нормативно-технической документации, за соблюдением установленного порядка выполнения работ, а также действующего законодательства при решении вопросов, касающихся защиты информации и координации деятельности подразделений по защите информации в Учреждении.

4.2. Установка перечня должностных групп, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- 4.3. Обеспечение отдельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- 4.4. Обеспечение пропускного режима в соответствии с утвержденными документами по охране и осуществлению пропускного режима;
- 4.5. Помещения, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;
- 4.6. Доступ к информации в электронном виде должен осуществляться с использованием парольной защиты, а в информационных системах персональных данных - с использованием средств автоматизации в соответствии с нормативными документами;
- 4.7. Осуществление внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 4.8. Ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников;
- 4.9. Выбор и реализация методов и способов защиты информации в информационных системах осуществляются на основе определяемых Учреждением угроз безопасности персональных данных (частной модели угроз) и, в зависимости от уровня защищенности информационной системы, определенного в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Приказом ФСТЭК России от 11.02.2013 № 17. Выбранные и реализованные методы и способы защиты информации в информационных системах должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе системы защиты персональных данных;
- 4.10. Учет машинных носителей персональных данных;
- 4.11. Выявление фактов несанкционированного доступа к персональным данным и принятие соответствующих мер;
- 4.12. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 4.13. Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных. Применение политики доступа к данным и аудита осуществляется с помощью встроенных средств операционных систем семейства Windows (технология Active Directory);
- 4.14. Персональные данные, обработка которых осуществляется в целях, несовместимых между собой, должны обрабатываться в различных, разделенных между собой межсетевыми экранами, сегментах локальной сети. Доступ в локальные сегменты сети Учреждения контролируется межсетевыми экранами, журналы работы которых должны регулярно

анализироваться с целью выявления попыток несанкционированного доступа. Используемые межсетевые экраны должны соответствовать требованиям руководящих документов ФСТЭК РФ по 3 уровню контроля на отсутствие НДВ и 3 классу защищенности для межсетевых экранов, а также требованиям ФСБ России к средствам криптографической защиты информации класса КС1 и возможностью применения для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну;

4.15. Контроль доступа и перемещений работников, пациентов и посетителей Учреждения с помощью систем видеонаблюдения и круглосуточным их мониторингом сотрудниками службы вневедомственной охраны;

4.16. Контроль доступа и фиксация перемещений работников в специальные служебные помещения с использованием системы контроля и управления доступа при помощи бесконтактных карт – идентификаторов. Система определяет права доступа в помещения согласно категории доступа для каждого работника;

4.17. Выдача бесконтактных карт – идентификаторов осуществляется уполномоченными сотрудниками Учреждения согласно категории доступа должностной группы;

4.18. На всех рабочих станциях иметь регулярно обновляемое антивирусное программное обеспечение;

4.19. Соблюдать регламентированную процедуру копирования документов, четко определяющую порядок создания копий на бумажных и электронных носителях и их дальнейшее использование;

4.20. Информацию, содержащую персональные данные, централизованно хранить на серверах, доступ к которым строго ограничить и регламентировать;

4.21. Контроль за предпринимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных;

4.22. Обязанности должностных лиц, осуществляющих обработку и защиту персональных данных, а также их ответственность, определяются Политикой информационной безопасности информационных систем персональных данных ГУЗ ТО «Тульская областная клиническая больница», утвержденной приказом руководителя Учреждения №130 от 04.09.2018.

## **5. Категории обрабатываемых персональных данных.**

5.1. Информация о персональных данных собирается исключительно с письменного согласия на обработку персональных данных субъекта персональных данных или его законного представителя, за исключением случаев прямо предусмотренных действующим законодательством РФ. При отказе субъекта персональных данных дать письменное согласие ему объясняются последствия такого отказа.

Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях.

## **6.1. Персональные данные пациента**

6.1.1. В состав персональных данных пациентов Учреждения входит следующая информация:

фамилия, имя, отчество, год, месяц, дата и место рождения, серия и номер паспорта, адрес регистрации и фактического проживания, идентификационный номер налогоплательщика (ИНН), страховое свидетельство государственного пенсионного страхования (СНИЛС), семейное, социальное положение, образование, профессия, должность, специальность, серия и номер страхового медицинского полиса и его действительность, номер амбулаторной карты, номер истории болезни, сведения о состоянии здоровья, в том числе группа здоровья, группа инвалидности и степень ограничения к трудовой деятельности, состояние диспансерного учета, зарегистрированные диагнозы по результатам обращения пациентов к врачу, в том числе при прохождении диспансеризации и медицинских осмотров, информация об оказанных медицинских услугах, в том числе о проведенных лабораторных анализах и исследованиях и их результатах, выполненных оперативных вмешательствах, случаях стационарного лечения и их результатах, о выданных листах временной нетрудоспособности с указанием номера листа нетрудоспособности и периода нетрудоспособности, регистрация прикрепления на территории обслуживания пациента – дата и признак прикрепления, информация о выписанных и отпущенных лекарственных средствах и изделиях медицинского назначения, информация о наличии льгот (по категориям), о документах, подтверждающих право на льготу и право на льготное лекарственное обеспечение, дата и причина смерти гражданина в случае его смерти.

6.1.2. Пациент, как субъект персональных данных, в том числе специальной категории персональных данных, имеет право на получение сведений:

- об Операторе, о месте нахождения Оператора;
- о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных;
- на подтверждение факта обработки персональных данных Оператором, а также цели такой обработки;
- о способах обработки персональных данных, применяемые Оператором;
- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источник их получения;
- о сроках обработки персональных данных, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

6.1.3. Пациент также имеет право:

- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими,

недостовверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- доступа к своим персональным данным при личном обращении к представителю Оператора при наличии паспорта;
- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;
- оформить доверенность на право доступа к его персональным данным;
- принимать предусмотренные законом меры по защите своих прав.

## 6.2 Персональные данные работника

6.2.1. К персональным данным работника Учреждения относится следующая информация:

информация, содержащаяся в трудовой книжке, информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования, информация об образовании, квалификации или о наличии специальных знаний и подготовки, информация, содержащаяся в документах воинского учета, информация медицинского характера, информация, содержащаяся в приказах по личному составу, информация, содержащаяся в иных документах, представляемых работником, содержащих информацию, необходимую работодателю в связи с трудовыми отношениями.

6.2.2. 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).

6.2.3. При оформлении работника в Учреждение работником кадрового органа 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 льготах;
- сведения о месте жительства и контактных телефонах.

6.2.4. В кадровом органе создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

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 исследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

6.2.5. Работник, как субъект персональных данных, имеет право на получение сведений:

- об Операторе, о месте нахождения Оператора,
- о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных,
- на подтверждение факта обработки персональных данных Оператором, а также цели такой обработки;
- о способах обработки персональных данных, применяемые Оператором;
- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источник их получения;
- о сроках обработки персональных данных, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

6.2.6. Работник имеет право:

- требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- доступа к своим персональным данным при личном обращении к представителю Оператора при наличии паспорта;
- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;
- оформить доверенность на право доступа к его персональным данным;
- принимать предусмотренные законом меры по защите своих прав.

6.2.7. Запрещается требовать от лица, поступающего на работу (или прием), документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

6.3. Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, дату и место рождения адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Учреждения, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись.

6.4. Персональные данные субъектов хранятся в электронных базах данных и на бумажных носителях в помещении отдела кадров Учреждения (регистратуре, архиве, медицинском отделении). Для этого используются специально оборудованные шкафы и сейфы. Личные дела уволенных (прошедших обследование, лечение) субъектов хранятся в архиве Учреждения.

## **7. Принципы обработки персональных данных учреждения.**

Обработка персональных данных ГУЗ ТО «ТОКБ» осуществляется на основе следующих принципов:

7.1. Учреждение в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона 152-ФЗ «О персональных данных».

7.2. Учреждение ограничивается достижением конкретных, заранее определённых и законных целей;

7.3. Обработке подлежат только персональные данные, которые отвечают целям их обработки;

7.4. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

7.5. Учреждение не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

7.6. Учреждение не производит трансграничную (на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.