

**ПРАВИЛА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И
ГРАЖДАН В ОГАУЗ «ИГКБ № 8»**

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила обработки персональных данных в ОГАУЗ «ИГКБ №8» (далее – Правила) устанавливают единый порядок обработки персональных данных работников и граждан, обращающихся в ОГАУЗ «ИГКБ № 8» (члены семьи, представители лиц, состоящих с учреждением в трудовых отношениях; физические лица, уволившиеся из учреждения; физические лица, являющиеся соискателями на вакантные должности; физические лица, состоящие с учреждением в гражданско-правовых отношениях; физические лица (пациенты), их законные представители, обратившиеся в учреждение за оказанием медицинской помощи; студенты, учащиеся образовательных медицинских учреждений, проходящие практику у Оператора; лица, осужденные к исправительным работам, именуемые в Правилах «граждане»).

1.2. Обработка персональных данных в ОГАУЗ «ИГКБ № 8» осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

1.3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом № 152-ФЗ.

1.4. Целью настоящих Правил является обеспечение защиты персональных данных работников и граждан от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

1.5. Настоящие Правила устанавливают и определяют:

- 1) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- 2) цели обработки персональных данных;
- 3) содержание обрабатываемых персональных данных для каждой цели обработки персональных данных;
- 4) категории субъектов, персональные данные которых обрабатываются;
- 5) сроки обработки и хранения обрабатываемых персональных данных;
- 6) порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований.

1.6. Основные условия обработки персональных данных:

1.6.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных, а именно:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных пунктами 2-7, 9-11 части 1 статьи 6 Федерального закона № 152-ФЗ.
- после направления уведомления об обработке персональных данных в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по Иркутской области, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона №152-ФЗ.
- после принятия Оператором необходимых мер по защите персональных данных.

1.6.2. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящими Правилами и подписывают обязательство о неразглашении информации.

II. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации:

2.2. Информационные ресурсы, содержащие персональные данные, созданные, приобретенные, накопленные в ОГАУЗ «ИГКБ № 8», а также полученные путем иных установленных законом способов, являются собственностью ОГАУЗ «ИГКБ № 8» и не могут быть использованы иначе, как в установленных законом случаях.

2.3. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

- назначение ответственного за организацию обработки персональных данных в ОГАУЗ «ИГКБ № 8»;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона №152-ФЗ;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- оценка вреда, который может быть причинён субъектам персональным данным в случае нарушения законодательства Российской Федерации и настоящих Правил;

- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных и настоящими Правилами;
- запрет на обработку персональных данных лицами, не допущенными к их обработке;
- запрет на обработку персональных данных под диктовку.

2.4. Документы, определяющие политику в отношении обработки персональных данных, подлежат обязательному опубликованию на официальном сайте ОГАУЗ «ИГКБ № 8» в течение 10 дней после их утверждения.

2.5. За разглашение информации, содержащей персональные данные, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение режима защиты, обработки и порядка использования этой информации, работник ОГАУЗ «ИГКБ № 8» может быть привлечен к дисциплинарной или иной ответственности, предусмотренной действующим законодательством РФ.

2.6. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации:

2.6.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации ОГАУЗ «ИГКБ № 8» осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

2.6.2. При эксплуатации автоматизированных информационных систем необходимо соблюдать следующие требования:

- к работе с персональными данными допускаются только лица, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных обязанностей; перечень должностей, допущенных к обработке персональных данных, определен соответствующим приказом главного врача;
- на персональных электронных вычислительных машинах (далее – ПЭВМ), дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);
- на период обработки защищаемой информации в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации;

- допуск других лиц в указанный период может осуществляться с разрешения главного врача или его заместителя, отвечающего за защиту информации.

2.6.3. Руководители структурных подразделений, работники ОГАУЗ «ИГКБ № 8» осуществляющие обработку персональных данных (далее - пользователи) обязаны контролировать и выполнять предусмотренные в ОГАУЗ «ИГКБ № 8» меры по защите информации, содержащей персональные данные.

2.6.4. Руководители структурных подразделений обязаны:

- участвовать в подготовке перечня персональных данных, обрабатываемых на ПЭВМ подразделения;
- готовить к утверждению списки работников, которых по своим должностным обязанностям необходимо допустить к работе с персональными данными в информационной системе ОГАУЗ «ИГКБ № 8»;
- контролировать целевое использование работниками ресурсов сети «Интернет»;
- контролировать выполнение пользователями общих правил работы на ПЭВМ и в локальной вычислительной сети ОГАУЗ «ИГКБ № 8» (далее – ЛВС);
- выборочно контролировать характер исходящей информации, направляемой пользователями по электронной почте другим адресатам и принимать оперативные меры к соблюдению ими установленных требований по защите персональных данных;
- при обнаружении нарушений установленных требований по защите персональных данных, в результате которых вскрыты факты их разглашения, прекратить работы на рабочем месте, где обнаружены нарушения, доложить главному врачу и поставить в известность начальника информационно-аналитического отдела.
- назначать служебные расследования по фактам разглашения информации, содержащей персональные данные, или утери документов, содержащих такую информацию, по фактам нарушений пользователями правил, установленных для работы с персональными данными в ЛВС, а также нарушений требований по защите информации;
- обеспечивать условия для работы представителя информационно-аналитического отдела при проверке в подразделении эффективности предусмотренных мер защиты информации;
- определять порядок передачи информации, содержащей персональные данные, другим подразделениям, сторонним организациям и органам.

2.6.5. При приеме на работу работник предупреждается об ответственности за разглашение сведений, содержащих персональные данные, которые станут ему известными в связи с предстоящим выполнением своих служебных обязанностей.

2.6.7 Пользователь обязан:

- знать правила работы в ЛВС и принятые меры по защите ресурсов ЛВС (в части, его касающейся);
- при работе на своей рабочей станции (ПЭВМ) и в ЛВС выполнять только служебные задания;
- перед началом работы на ПЭВМ проверить свои рабочие папки на жестком магнитном диске, съемные магнитные носители информации на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности своей рабочей станции;
- при сообщениях программ о появлении вирусов немедленно прекратить работу, доложить начальнику информационно-аналитического отдела (специалисту информационно-аналитического отдела) и своему непосредственному руководителю;
- при обработке информации, содержащей персональные данные, использовать только зарегистрированные в журналах учета машинные носители информации (далее – МНИ);
- при необходимости использования неучтенных магнитных носителей, прежде всего, провести проверку этих носителей на отсутствие вирусов;
- выполнять предписания работника информационно-аналитического отдела ответственного за защиту информации в ОГАУЗ «ИГКБ № 8»;
- представлять для контроля свою рабочую станцию (ПЭВМ) работникам информационно-аналитического отдела;
- сохранять в тайне свой индивидуальный пароль, периодически, но не реже чем один раз в полгода, изменять его и не сообщать другим лицам;
- вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;
- при обнаружении различных неисправностей в работе компьютерной техники или ЛВС, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить в информационно-аналитического отдела, администратору сети и поставить в известность руководителя подразделения.

Пользователю при работе запрещается:

- играть в компьютерные игры;
- приносить различные компьютерные программы и пытаться установить их на локальный диск компьютера без уведомления специалистов информационно-аналитического отдела;
- перенастраивать программное обеспечение компьютера;
- самостоятельно вскрывать комплектующие рабочей станции (ПЭВМ);
- запускать на своей рабочей станции (ПЭВМ) или другой рабочей станции сети любые системные или прикладные программы, кроме

установленных специалистами отдела информатизации и защиты информации сети;

- изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла;
- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), магнитные носители и распечатки, содержащие персональные данные;
- допускать к подключенной в сеть рабочей станции (ПЭВМ) посторонних лиц;
- производить копирование для временного хранения информации, содержащей персональные данные, на неучтенные носители;
- работать на рабочей станции (ПЭВМ) в сети с информацией, содержащей персональные данные, при обнаружении неисправностей станции (ПЭВМ), влияющих на защиту информации;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к утечке, блокированию, искажению или утере информации, содержащей персональные данные;
- отправлять по электронной почте информацию для решения личных проблем, а также информацию по просьбе третьих лиц без согласования с начальником отдела;
- запрашивать и получать из сети "Интернет" материалы развлекательного характера (игры, клипы и т.д.);
- запрашивать и получать из сети "Интернет" программные продукты, кроме случаев, связанных со служебной необходимостью. При этом необходимо согласование с начальником отдела и обеспечение процесса техническими специалистами отдела информатизации и защиты информации.

2.6.8. Работники не могут использовать в личных целях персональные данные, ставшие известными им вследствие выполнения служебных обязанностей.

2.7. Порядок обработки персональных данных без использования средств автоматизации:

2.7.1. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

2.7.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

2.7.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

2.7.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных (при необходимости получения письменного согласия на обработку персональных данных);
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

2.7.5. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в закрываемых шкафах, тумбочках (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность. Работа с информационными системами персональных данных, материальными носителями, в том числе с медицинской документацией, содержащими персональные данные пациентов осуществляется в специально отведённых

для этого помещениях: ординаторские, кабинеты врачей, орг.-метод. отделы, кабинет медицинской статистики, регистратуры, серверная и т.д.

2.7.6. 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).

2.8. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных - осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных - уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

2.9. 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.

2.10. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

2.11. Необходимо обеспечивать отдельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

III. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Целью обработки персональных данных является:

Обеспечения организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами «Об обязательном медицинском страховании граждан в Российской Федерации» от 29 ноября 2010 года № 326-ФЗ и «Об основах охраны здоровья граждан Российской Федерации» от 21 ноября 2011г № 323-ФЗ.

Обработка Оператором персональных данных пациента осуществляется исключительно в целях оказания пациенту качественной медицинской помощи (услуг) в необходимых объёмах, соблюдения требований действующего законодательства, иных нормативных правовых актов, обеспечения контроля объёмов и качества оказанной медицинской помощи (услуг).

Осуществления трудовых отношений, кадрового и бухгалтерского учета, награждения и поощрения сотрудников, осуществления подготовки и повышения квалификации кадров, по вопросу оказания амбулаторной и стационарной помощи населению; прохождения практики студентами и учащимися медицинских образовательных учреждений; отбывания наказания лицами, осужденными к исправительным работам.

Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения требований действующего законодательства, иных нормативных правовых актов, обучении и продвижении по службе, обеспечения личной безопасности работников, обеспечения контроля количества и качества выполняемой работы, развития организации, обеспечения сохранности имущества, соблюдения пропускного режима.

Осуществление гражданско-правовых отношений, в том числе договорных отношений с физическими лицами при оказании медицинских услуг.

IV. ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Получение персональных данных преимущественно осуществляется путем представления их самим гражданином, на основании его письменного согласия, за исключением случаев прямо предусмотренных действующим законодательством РФ.

В случаях, предусмотренных Федеральным законодательством, обработка персональных данных осуществляется только с согласия гражданина в письменной форме. Равнозначным содержащему собственноручную подпись гражданина согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом № 152-ФЗ электронной подписью. Согласие гражданина в письменной форме на обработку его персональных данных должно включать в себя, в частности:

- 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- 3) наименование или фамилию, имя, отчество и адрес Управления, получающего согласие субъекта персональных данных;
- 4) цель обработки персональных данных;
- 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Управления, если обработка будет поручена такому лицу;
- 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Управлением способов обработки персональных данных;
- 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законодательством;
- 9) подпись субъекта персональных данных.

Для обработки персональных данных, содержащихся в согласии в письменной форме на обработку его персональных данных, дополнительное согласие не требуется.

4.2. В случае необходимости проверки персональных данных гражданина заблаговременно должно сообщить об этом гражданину, о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа гражданина дать письменное согласие на их получение.

4.3 Обработка персональных данных работника не требует получения соответствующего согласия в следующих случаях:

- 1) Если объем обрабатываемых работодателем персональных данных не превышает установленные перечни, а также соответствует целям обработки, предусмотренным трудовым законодательством, пенсионным, налоговым законодательством.
- 2) В случаях, предусмотренных правилами внутреннего трудового распорядка, а также локальными актами работодателя, принятыми в порядке, установленном ст. 372 Трудового кодекса РФ.
- 3) Обязанность по обработке, в том числе опубликованию и размещению персональных данных работников в сети Интернет, предусмотрена законодательством Российской Федерации.

4) Обработка персональных данных близких родственников работника в объеме, предусмотренном унифицированной формой № Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат). В иных случаях, получение согласия близких родственников работника является обязательным условием обработки их персональных данных.

5) Обработка специальных категорий персональных данных работника, в том числе, сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения работником трудовой функции на основании положений п. 2.3 ч. 2 ст. 10 Федерального закона «О персональных данных» в рамках трудового законодательства.

6) Обработка необходима для защиты жизни и здоровья работника, гражданина, если получение согласия невозможно.

7) При передаче его персональных данных в случаях, связанных с выполнением им должностных обязанностей, в том числе, при его командировании (в соответствии с Правилами оказания гостиничных услуг в Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 25.04.1997 № 490, нормативными правовыми актами в сфере транспортной безопасности).

8) В случаях передачи работодателем персональных данных работников в налоговые органы, военные комиссариаты, профсоюзные органы, предусмотренные действующим законодательством Российской Федерации.

9) При мотивированных запросов от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

В случае поступления запросов из организаций, не обладающих соответствующими полномочиями, работодатель обязан получить согласие работника на предоставление его персональных данных и предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что это правило будет (было) соблюдено.

10) Передача персональных данных работника кредитным организациям, открывающим и обслуживающим платежные карты для начисления заработной платы, осуществляется без его согласия в следующих случаях:

- договор на выпуск банковской карты заключался напрямую с работником и в тексте, которого предусмотрены положения, предусматривающие передачу работодателем персональных данных работника;
- наличие у работодателя доверенности на представление интересов работника при заключении договора с кредитной организацией на выпуск банковской карты и ее последующем обслуживании;
- соответствующая форма и система оплаты труда прописана в локальных актах Оператора.

11) Обработка персональных данных работника при осуществлении пропускного режима на территорию служебных зданий и помещений работодателя, при условии, что организация пропускного режима осуществляется работодателем самостоятельно либо если указанная обработка соответствует порядку, предусмотренному локальными актами работодателя, принятыми в соответствии со ст. 372 Трудового кодекса РФ.

4.4 Обработка персональных данных соискателей на замещение вакантных должностей в рамках правоотношений, урегулированных Трудовым кодексом РФ, предполагает получение согласия соискателей на замещение вакантных должностей на обработку их персональных данных на период принятия работодателем решения о приеме либо отказе в приеме на работу.

Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым данное лицо заключил соответствующий договор, при самостоятельном размещении соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц, а также при направлении соискателем своего резюме на электронную почту должностного лица ОГАУЗ «ИГКБ № 8».

При поступлении в адрес работодателя резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо его направившее не представляется возможным, данное резюме подлежит уничтожению в день поступления.

В случае, если сбор персональных данных соискателей осуществляется посредством типовой формы анкеты соискателя, утвержденной оператором, то данная типовая форма анкеты должна соответствовать требованиям п. 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, а также содержать информацию о сроке ее рассмотрения и принятия решения о приеме либо отказе в приеме на работу.

В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней. Получение согласия также является обязательным условием при направлении

работодателем запросов в иные организации, в том числе, по прежним местам работы, для уточнения или получения дополнительной информации о соискателе.

V. СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При поступлении на работу работник предоставляет персональные данные о себе в документированной форме. А именно:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний при поступлении на работу, требующую специальных знаний или специальной подготовки;
- в отдельных случаях с учетом специфики работы действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов (например, медицинское заключение для лиц в возрасте моложе 18 лет; для лиц, занятых на тяжелых работах и работах с вредными и (или) опасными условиями труда, а также на работах, связанных с движением транспорта), справку об отсутствии судимости, при приеме для работы в детской поликлинике.
- свидетельство о постановке на учет физического лица (ИНН).

5.2. При заключении трудового договора и в ходе трудовой деятельности может возникнуть необходимость в предоставлении работником документов, содержащих персональные данные:

- о возрасте детей;
- об инвалидности;
- о донорстве;
- о составе семьи;
- о доходе с предыдущего места работы;
- о необходимости ухода за больным членом семьи;
- прочие.

5.3. После того, как будет принято решение о приеме работника на работу, а также в процессе трудовой деятельности к документам, содержащим персональные данные работника, будут относиться:

- трудовой договор и приказ о приеме на работу;
- автобиография;
- приказы о поощрениях и взысканиях;
- приказы об изменении условий трудового договора;
- карточка унифицированной формы Т-2, утвержденная Постановлением Госкомстата России от 05.01.04 № 1;

- личное дело работника;
- лицевые счета работников.

5.4. К персональным данным работников, соискателей на вакантную должность, относятся:

- 1) биографические данные гражданина, адрес регистрации по месту жительства и фактического проживания;
- 2) паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи, наименование органа, выдавшего документ);
- 3) сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (включая серию, номер, дату выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дату начала и завершения обучения);
- 4) сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовках;
- 5) сведения о номере, серии, дате выдачи трудовой книжки (вкладыша в неё) и записях в ней, содержание и реквизиты трудового договора (контракта);
- 6) сведения о составе семьи и наличии иждивенцев;
- 7) сведения о состоянии здоровья и наличии заболеваний (когда это необходимо в случаях, установленных законом);
- 9) сведения об отношении к воинской обязанности;
- 10) сведения об идентификационном номере налогоплательщика;
- 11) сведения о социальных льготах и о социальном статусе;
- 12) сведения из страховых полисов обязательного медицинского страхования;
- 13) сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

5.5. При обращении к оператору для получения медицинской помощи граждане, их представители предъявляет регистраторам следующие документы, содержащие персональные данные:

- паспорт или иной документ, удостоверяющий личность, содержащий сведения о месте регистрации (месте жительства);
- страховое свидетельство фонда ОМС, страховой компании, содержащее сведения о номере и серии страхового свидетельства.

5.6. К персональным данным граждан, обратившихся для получения медицинской помощи относятся:

- 1) фамилия, имя, отчество;
- 2) пол;
- 3) дата рождения;
- 4) место рождения;
- 5) гражданство;
- 6) данные документа, удостоверяющего личность;
- 7) место жительства;
- 8) место регистрации;

9) страховой номер индивидуального лицевого счета (СНИЛС), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;

10) номер полиса обязательного медицинского страхования застрахованного лица;

11) данные о страховой медицинской организации, выбранной застрахованным лицом;

12) дата регистрации в качестве застрахованного лица;

13) статус застрахованного лица (работающий, неработающий), место работы учебы;

14) виды оказанной медицинской помощи;

15) условия оказания медицинской помощи;

16) сроки оказания медицинской помощи;

17) объемы оказанной медицинской помощи;

18) стоимость оказанной медицинской помощи;

19) диагноз;

20) профиль оказания медицинской помощи;

21) медицинские услуги, оказанные застрахованному лицу, и примененные лекарственные препараты;

22) примененные медико-экономические стандарты;

23) результат обращения за медицинской помощью;

24) результаты проведенного контроля объемов, сроков, качества и условий предоставления медицинской помощи.

25) сведения о факте, времени, частоте обращений в медицинскую организацию;

26) сведения о состоянии здоровья, история болезни

VI. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

6.1. К субъектам, персональные данные которых обрабатываются, относятся:

-физические лица, состоящие с учреждением в трудовых отношениях;

- члены семей лиц, представители лиц, состоящих с учреждением в трудовых отношениях;

-физические лица, уволившиеся из учреждения;

-физические лица, являющиеся соискателями на вакантные должности;

-физические лица, состоящие с учреждением в гражданско-правовых отношениях;

-физические лица, их законные представители, обратившиеся в учреждение за оказанием медицинской помощи;

-физические лица, обратившиеся в учреждение с запросами, жалобами и иными обращениями;

-студенты, учащиеся образовательных медицинских учреждений, проходящие практику у Оператора;

-лица, осужденные к исправительным работам.

VII. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ ТРЕТЬИМ ЛИЦАМ

7.1. Передача персональных данных пациентов третьим лицам осуществляется только с письменного согласия пациента, с подтверждающей визой главного врача, за исключением случаев, предусмотренных ст. 13 Федерального закона РФ от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учётом положений пункта 1 части 9 статьи 20 указанного Федерального закона;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 указанного Федерального закона, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 указанного Федерального закона, для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинён в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с указанным Федеральным законом.

VIII. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Порядок хранения документов, содержащих персональные данные осуществлять в соответствии с:

- Правилами, устанавливающими порядок ведения и хранения трудовых книжек, а также порядок изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденными Постановлением Правительства РФ от 16 апреля 2003 г. № 225 «О трудовых книжках» (в ред. от 06 февраля 2004 г.);
- Унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными Постановлением Госкомстата России от 05 января 2004 г. № 1;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным Приказом Минкультуры России от 25 августа 2010 г. № 558.
- сроками хранения медицинской документации (письмо Минздрава РФ от 07.12.2015г. № 13-2/1538).

Работодатель вправе обрабатывать без согласия ПД уволенных работников в случаях и сроки, предусмотренные по ФЗ РФ:

- а) в соответствии с ст.24 Налогового кодекса – 4 года (нужно обеспечить сохранность документов для исчисления, удержания и перечисления налогов;
- б) в соответствии с ФЗ «О бухгалтерском учете» организации обязаны хранить бухгалтерскую документацию не менее 5 лет.
- 3) в случае отказа в приеме на работу, сведения соискателя должны быть уничтожены в течении 30 дней.
- 4) иными требованиями законодательства Российской Федерации.

8.2. Особенности хранения персональных данных:

Если срок хранения персональных данных не установлен законодательством Российской Федерации, нормативными правовыми актами ОГАУЗ «ИГКБ № 8» или договором, стороной которого или поручителем по которому является субъект персональных данных, то хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

XI. ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных, или в результате которых уничтожаются материальные носители персональных данных.

9.2. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

9.3. Порядок уничтожения обработанных персональных данных.

- Уничтожению подлежат утратившие практическое значение и не имеющие исторической или иной ценности носители информации, содержащие персональные данные. При уничтожении таких носителей должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.
- Уничтожение производится путем сожжения, расплавления, дробления, растворения, химического разложения или превращения в мягкую бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в бумажную сечку. Магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и другими способами, исключающими возможность их восстановления.
- Уничтожение обработанных персональных данных производится комиссионно, с составлением соответствующего акта. Состав комиссии назначается приказом главного врача. В комиссию назначаются лица, допущенные к работе с персональными данными и имеющие непосредственное отношение к уничтожаемым материалам.
- На документальные материалы, отобранные комиссией для уничтожения, составляется акт об уничтожении документов, который подписывается членами комиссии и утверждается главным врачом.
- Отобранные и включенные в акт об уничтожении документальные материалы после их сверки членами комиссии хранятся отдельно от других материалов.
- Уничтожение документальных материалов до утверждения акта об уничтожении документов главным врачом запрещается.
- Уничтожение должно производиться в возможно короткий срок после утверждения главным врачом акта об уничтожении документов.

9.4. Без оформления акта уничтожаются: испорченные бумажные и технические носители, черновики и проекты документов и другие материалы, образовавшиеся при исполнении документов, содержащих персональные данные.

В процедуру уничтожения документов и носителей информации без составления акта входит проведение следующих мероприятий:

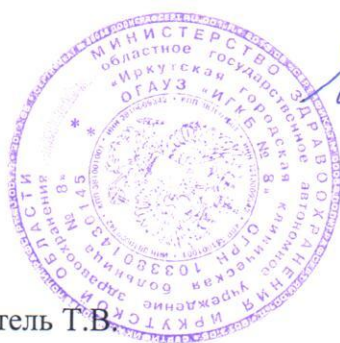
- разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя и руководителя подразделения, допущенных к обработке персональных данных;
- накапливание остатков носителей в печатаемом ящике (урне);
- физическое уничтожение остатков носителей несколькими сотрудниками подразделения, допущенными к работе с персональными данными;
- внесение отметок об уничтожении в учетные формы документов и носителей.

Х. ОТВЕТСТВЕННОСТЬ

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

10.2. Лица организации, получившие в установленном порядке доступ к персональным данным работника, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника привлекаются работодателем к дисциплинарной ответственности в порядке предусмотренной ст.192, 193 Трудового кодекса Российской Федерации, в исключительных случаях подлежат увольнению по подпункту В пункта 6 части первой статьи 81 Трудового кодекса РФ – разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей.

Главный врач



Ж.В. Есева

Исполнитель:

Юрисконсульт Бартель Т.В.