



«Утверждаю»:
Главный врач
/ И.О. Феклина/

ПОЛИТИКА ГУЗ «ЕЛЕЦКАЯ ГОРОДСКАЯ БОЛЬНИЦА №2» В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. Общие положения. Основные понятия

1. Политика в отношении обработки персональных данных субъектов в ГУЗ «Елецкая городская больница №2» (далее по тексту – Политика) разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Рекомендациями Роскомнадзора по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ О персональных данных», целях соблюдения требований законодательства РФ в сфере персональных данных и направлена на регулирование отношений по обработке и защите персональных данных субъектов в ГУЗ «Елецкая городская больница №2».

2. Настоящая Политика размещается на официальном сайте ГУЗ «Елецкая городская больница №2» в информационно-телекоммуникационной сети «Интернет» по адресу: <http://больница2.рф/> в соответствующем разделе сайта.

3. Основные понятия, используемые в Политике:

1) персональные данные – информация, относящаяся прямо или косвенно к определённому или определяемому лицу.

2) оператор персональных данных (оператор) – ГУЗ «Елецкая городская больница №2» (Оператор, Учреждение), самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) субъект персональных данных – лицо, предоставляющее свои персональные данные оператору;

4) обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);

- обезличивание;
- блокирование;
- удаление;
- уничтожение.

5) автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

6) распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

7) предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или кругу лиц;

8) блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

9) уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

10) обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

11) информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

12) информация – сведения (сообщения, данные) независимо от формы их представления;

13) документированная информация – зафиксированная на материальном носителе путём документирования информация с реквизитами, позволяющими определить такую информацию или её материальный носитель;

14) доступ к информации – возможность получения информации и её использования;

15) угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

II. Сбор (получение) и хранение персональных данных

1. По общему правилу все персональные данные Оператор получает у Субъекта персональных данных. Если персональные данные возможно получить только у третьей стороны, то Субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

2. Оператор должен сообщить Субъекту о целях, предполагаемых источниках и способах получения персональных данных, о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

3. Обязанности Оператора при сборе персональных данных:

- при сборе персональных данных предоставить Субъекту по его просьбе необходимую информацию, касающуюся обработки его персональных данных;

- если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить Субъекту юридические последствия отказа предоставить свои персональные данные;

- если персональные данные получены не от Субъекта, Оператор до начала обработки таких персональных данных обязан предоставить ему следующую информацию:

- 1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- 2) цель обработки персональных данных и её правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные законом права субъекта персональных данных;
- 5) источник получения персональных данных.

Оператор освобождается от обязанности предоставить Субъекту вышеуказанные сведения, в случаях, если:

1) Субъект уведомлён об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными Субъектом или получены из общедоступного источника;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления научной или иной творческой деятельности, если при этом не нарушаются права и законные интересы Субъекта;

5) предоставление Субъекту таких сведений, нарушает права и законные интересы третьих лиц.

- не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта, если иное не предусмотрено федеральным законом;

- при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных Субъектов с использованием баз данных, находящихся на территории России;

4. Требования к помещениям и оборудованию, где хранятся (обрабатываются) персональные данные:

1) Персональные данные хранятся на материальных (бумажных и электронных) носителях в специально предназначенных для этого помещениях, шкафах или сейфах, на компьютерах сотрудников, уполномоченных на работу с персональными данными, а также в информационных системах.

2) Помещения, в которых хранятся материальные носители, содержащие персональные данные, оборудуются надежными замками и сигнализацией, а шкафы (сейфы) – замками, а также при необходимости – пломбами.

3) Расположение помещений, шкафов, сейфов, компьютеров должно исключать возможность несанкционированного проникновения в них посторонних лиц.

4) На компьютерах, содержащих системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.

5) Доступ к помещениям, шкафам, сейфам, компьютерам должен быть только у лиц, уполномоченных на работу с персональными данными. Указанные помещения в рабочее время при отсутствии в них лиц, уполномоченных на работу с персональными данными, должны быть закрыты. Доступ к компьютерам, а также в соответствующие информационные системы персональных данных осуществляется посредством введения индивидуальных логинов и паролей.

6) Внутренняя планировка и расположение рабочих мест в помещениях должны обеспечивать сохранность доверенных работникам конфиденциальных документов и сведений, содержащих персональные данные.

7) Допуск в помещения вспомогательного и обслуживающего персонала (уборщицы, электромонтеры, сантехники и т.д.) производится только при служебной необходимости и в сопровождении ответственного за помещение, при этом необходимо принять меры, исключающие визуальный просмотр конфиденциальных документов, содержащих персональные данные.

8) По окончании рабочего дня выделенные помещения закрываются и при необходимости опечатываются.

5. В процессе хранения персональных данных должны обеспечиваться:

- требования законов и иных нормативных правовых актов, устанавливающих правила хранения таких сведений;

- условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ, в соответствии с законодательством РФ и настоящим Положением;

- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

6. Обработка персональных данных 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 данных либо имеющих к ним доступ.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

III. Обработка персональных данных

1. Оператор самостоятельно определяет объём, содержание обрабатываемых персональных данных, устанавливает способы обработки персональных данных в зависимости от целей такой обработки и материально-технических возможностей учреждения, в соответствии с требованиями законодательства РФ.

Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Основные принципы обработки персональных данных:

а) Обработка персональных данных осуществляется на законной и справедливой основе.

б) Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями их сбора.

в) Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых между собой целях.

г) Обработке подлежат только персональные данные, которые отвечают целям их обработки.

д) Содержание и объём обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

е) При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях – актуальность по отношению к целям их обработки. Оператор принимает необходимые меры по удалению или уточнению неполных или неточных данных.

2. Оператор и его уполномоченные сотрудники при обработке персональных данных обязаны соблюдать следующие требования:

а) при определении объема и содержания обрабатываемых персональных данных следует руководствоваться Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

б) оператор, а также его уполномоченные работники обязаны соблюдать врачебную тайну, в том числе конфиденциальность персональных данных пациентов, используемых в медицинских информационных системах;

в) обработка персональных данных в информационных системах в сфере здравоохранения осуществляется с соблюдением требований, установленных законодательством РФ в области персональных данных, и соблюдением врачебной тайны.

г) нельзя получать и обрабатывать сведения о субъекте, относящиеся в соответствии с законодательством РФ в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных федеральными законами;

д) нельзя получать и обрабатывать персональные данные Субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами;

е) при принятии решений, затрагивающих интересы Субъекта, нельзя основываться на его персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения;

ж) обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни Субъекта, не допускается, за исключением случаев, установленных в ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Обработка персональных данных осуществляется исключительно уполномоченными сотрудниками Оператора, непосредственно использующими эти данные в служебных целях. Уполномоченные сотрудники имеют право получать только те персональные данные Субъектов, которые необходимы для надлежащего выполнения ими своих должностных обязанностей.

4. Сотрудники, осуществляющие работу с персональными данными в силу исполнения ими своих должностных обязанностей, обеспечивают защиту персональных данных Субъектов, содержащихся в их делах, медицинских картах, медицинской документации и иных документах, в автоматизированных информационных системах от неправомерного их использования. Уполномоченные сотрудники, которые имеют доступ к персональным данным других Субъектов, обязаны не разглашать эти данные, которые стали им известны в связи с выполнением ими трудовых обязанностей.

5. Персональные данные при их обработке должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

6. При фиксации персональных данных не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

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

а) при необходимости использования или распространения персональных данных отдельно от находящихся на том же материальном носителе других 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;

б) 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.

8. 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 таком носителе (удаление, вымарывание).

9. Уничтожение бумажных носителей (документов), содержащих персональные данные, осуществляется путём измельчения их на мелкие части (или иным способом), исключающим возможность последующего восстановления информации либо сжигаются. Уничтожение машинных носителей информации, содержащих персональные данные, осуществляются путём деформирования, нарушения единой целостности такого носителя. Подлежащие уничтожению файлы, расположенные на жестком диске компьютера, удаляются средствами специального программного обеспечения операционной системы с последующим «очищением корзины». В случае допустимости повторного использования носителя применяется программное удаление («затириание») содержимого путём его форматирования с последующей записью новой информации на данный носитель. Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом главного врача. Комиссия составляет и подписывает Акт об уничтожении носителей, который хранится в сейфе у руководителя соответствующего подразделения.

10. Оператор обязан прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, действующим по поручению Оператора:

- в случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, в срок, не превышающий трех рабочих дней с даты этого выявления;

- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператором;

- в случае достижения цели обработки персональных данных и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

IV. Передача персональных данных третьим лицам

1. Оператор вправе передавать персональные данные Субъекта третьей стороне только с письменного согласия Субъекта (его законного представителя), за исключением установленным федеральным законом случаев.

2. Согласие Субъекта на предоставление его персональных данных третьим лицам не требуется в следующих случаях:

- при поступлении официальных запросов (письменного запроса на бланке организации с печатью и росписью руководителя) из правоохранительных, надзорных, контрольных органов (суд, органы прокуратуры, ФСБ, МВД и т.д., и т.п.);

- при непосредственном обращении сотрудников правоохранительных, надзорных, контрольных органов при предъявлении ими служебного удостоверения и соответствующих документов о получении персональных данных (запрос, постановление и т.п.), а также в иных случаях, предусмотренных федеральным законом;

- по требованию полномочных государственных органов – в случаях, предусмотренных федеральным законом;

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

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов пациента, если получение его согласия невозможно;

- персональные данные являются общедоступными.

3. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю (если медицинское вмешательство необходимо по экстренным показаниям для устранения угрозы жизни человека и если его состояние не позволяет выразить свою волю или отсутствуют законные представители);

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 органов прокуратуры в связи с осуществлением ими прокурорского надзора, 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;

3.1) в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

4) в случае оказания медицинской помощи несовершеннолетнему, больному наркоманией при оказании ему наркологической помощи или при медицинском освидетельствовании несовершеннолетнего в целях установления состояния наркотического либо иного токсического опьянения, а также несовершеннолетнему, не достигшему возраста 15-ти лет (для больных наркоманией – 16-ти лет), – 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 причинен 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 и федеральных государственных органов, 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 РФ о персональных данных;

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

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

4. С письменного согласия гражданина или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

5. Согласие на обработку персональных данных может быть отозвано Субъектом в любое время на основании его личного заявления, поданного на имя главного врача.

6. Субъект, о котором запрашиваются сведения, относящиеся к персональным данным, должен быть уведомлён о передаче его персональных данных третьим лицам.

7. Оператор не осуществляет передачу персональных данных Субъектов на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу (трансграничную передачу персональных данных).

8. Обязанности Оператора (уполномоченных лиц) при обращении к нему (получении запроса) Субъекта или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

- сообщить в установленном порядке Субъекту или его представителю необходимую информацию о персональных данных, относящихся к нему, а также предоставить возможность ознакомления с этими персональными данными – в течение 30 дней с даты получения такого запроса. В случае отказа в предоставлении такой информации учреждение обязано дать в письменной форме мотивированный ответ;

- предоставить безвозмездно Субъекту (его представителю) возможность ознакомления с персональными данными, относящимися к нему;

- в срок, не превышающий 7 рабочих дней со дня предоставления Субъектом (его представителем) сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, учреждение обязано внести в них изменения;

- в срок, не превышающий 7 рабочих дней со дня представления Субъектом (его представителем) сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, учреждение обязано уничтожить такие персональные данные;

- уведомить Субъекта (его представителя) о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого Субъекта были переданы;

- сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа информацию в течение 30 дней с даты получения запроса.

V. Меры по обеспечению безопасности персональных данных

1. Оператор обязан принимать необходимые и достаточные правовые, организационные и технические меры (обеспечивать их принятие) для защиты персональных данных Субъектов 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 Субъектов.

Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных

данных» и принятыми в соответствии с ним нормативными правовыми актами. Состав и перечень мер оператор определяет самостоятельно.

2. Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности Оператора.

3. Помимо мер и требований, указанных в других разделах настоящего документа, для обеспечения внешней и внутренней защиты персональных данных Субъектов Оператор принимает, в частности, следующие меры:

- устанавливает пропускной режим в учреждение и особый порядок приёма, учёта и контроля деятельности посетителей;
- использует технические средства охраны;
- использует программно-технический комплекс защиты информации на электронных носителях (установка антивирусного программного обеспечения на компьютеры сотрудников, работающих с персональными данными, и выдача индивидуальных логинов и паролей для доступа к компьютерам, а также в соответствующие информационные системы персональных данных);
- регламентирует состав работников, функциональные обязанности которых требуют доступа к персональным данным, и имеющих право доступа (входа) в помещения, в которых хранятся персональные данные;
- принимает меры по недопущению неконтролируемого (несанкционированного) проникновения в помещения, в которых находятся персональные данные или доступ к информационным системам персональных данных;
- обеспечивает сохранность материальных носителей персональных данных;
- избирательно и обоснованно распределяет документы и информацию, содержащую персональные данные, между лицами, уполномоченными на работу с такими данными;
- рационально размещает рабочие места для исключения бесконтрольного доступа к персональным данным;
- создаёт необходимые условия для работы с документами и базами данных, содержащими персональные данные Субъектов;
- своевременно выявляет и устраняет нарушения установленных требований по защите персональных данных Субъектов;
- регулярно проверяет знание работниками, имеющими отношение к работе с персональными данными, требований нормативно-методических документов по защите таких данных;
- организует порядок уничтожения информации;
- проводит профилактическую работу с должностными лицами, имеющими доступ к персональным данным, по предупреждению разглашения таких сведений.

4. Обеспечение безопасности персональных данных достигается, в частности:

- 1) определением угроз безопасности персональных данных при их обработке;
- 2) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- 3) установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учёта всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- 4) контролем за принимаемыми сотрудниками мерами по обеспечению безопасности персональных данных.

5. Оператор разрешает доступ к персональным данным Субъектов только специально уполномоченным сотрудникам, при этом указанным лицам будут доступны только те

персональные данные, которые необходимы для выполнения ими своих служебных обязанностей.

5.1. Конкретный перечень работников, которые имеют доступ к персональным данным, устанавливается приказом главного врача.

VI. Права и обязанности субъектов в сфере обработки персональных данных

1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, Субъект имеет право на:

1) получение полной информации о своих персональных данных и обработке этих данных, в том числе содержащую:

- обрабатываемые персональные данные, относящиеся к нему, источник их получения;
- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- порядок осуществления своих прав, предусмотренных федеральным законом и настоящим документом;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

- сроки обработки персональных данных, в том числе сроки их хранения;
- иные сведения, предусмотренные федеральным законом.

Указанные сведения должны быть предоставлены Субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим Субъектам, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Указанные сведения предоставляются Субъекту (его представителю) при письменном запросе в учреждение. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта (его представителя), сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта в отношениях с учреждением (номер договора, дата заключения договора), либо сведения, иным образом подтверждающие факт обработки персональных данных учреждением, подпись Субъекта (его представителя).

2) свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом;

3) обеспечение соблюдения требований конфиденциальности персональных данных, надлежащей их защиты;

4) определение своих представителей для защиты своих персональных данных;

5) доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

6) требование об исключении или исправлении неверных (неполных) персональных данных, а также данных, обработанных с нарушением требований федерального закона. При отказе учреждения исключить или исправить персональные данные Субъекта он имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера Субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

7) требование об извещении учреждением всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;

8) обжалование в суд любых неправомерных действий или бездействия учреждения при обработке и защите его персональных данных;

9) отзыв ранее данного согласия на обработку персональных данных в установленном порядке;

10) защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

2. Право Субъекта на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание Субъекта по подозрению в совершении преступления, либо предъявившими ему обвинение по уголовному делу, либо применившими к нему меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ Субъекта к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

3. Если Субъект считает, что Оператор осуществляет обработку его персональных данных с нарушением требований закона или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

4. Субъекты имеют и иные права касаясь своих персональных данных, предусмотренные законодательством РФ.

VII. Обязанности Оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных:

1. Если при обращении (по запросу) Субъекта (его представителя либо уполномоченного органа по защите прав субъектов персональных данных) была выявлена неправомерная обработка его персональных данных – Оператор обязан: *блокировать* такие персональные данные, относящиеся к этому Субъекту, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению) на период проверки; *прекратить неправомерную обработку* персональных данных или обеспечить прекращение неправомерной обработки данных лицом, действующим по поручению. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления факта, обязан *уничтожить* такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор

обязан уведомить Субъекта (его представителя; орган по защите прав субъектов персональных данных).

2. Если при обращении (по запросу) Субъекта (его представителя либо уполномоченного органа по защите прав субъектов персональных данных) были выявлены неточные персональные данные – Оператор обязан: *блокировать* такие персональные данные, относящиеся к этому Субъекту, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению) на период проверки, если блокирование персональных данных не нарушает права и законные интересы Субъекта или третьих лиц. В случае подтверждения факта неточности персональных данных учреждение на основании сведений, представленных Субъектом (его представителем либо уполномоченным органом по защите прав субъектов персональных данных), или иных документов обязано *уточнить* персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) в течение 7 рабочих дней со дня представления таких сведений и *снять блокирование* персональных данных.

3. В случае достижения цели обработки персональных данных Оператор обязан *прекратить обработку* персональных данных или обеспечить её прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) и *уничтожить* персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект, иным соглашением между учреждением и Субъектом либо если Оператор не вправе осуществлять обработку персональных данных без согласия Субъекта на основаниях, предусмотренных федеральным законом.

4. В случае отзыва Субъектом согласия на обработку его персональных данных Оператор обязан *прекратить их обработку* или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, *уничтожить* персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект, иным соглашением между Оператором и Субъектом либо если Оператор не вправе осуществлять обработку персональных данных без согласия Субъекта персональных данных на основаниях, предусмотренных федеральным законом;

5. В случае отсутствия возможности уничтожения персональных данных в течение вышеуказанного срока, Оператор осуществляет *блокирование таких персональных данных* или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению) и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

6. Оператор несёт также иные обязанности в сфере персональных данных, предусмотренные законодательством РФ.