

Политика в области обработки и обеспечения безопасности персональных данных в информационных системах персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»

ВВЕДЕНИЕ

1. Общие положения
2. Принципы, правила и цели обработки персональных данных
3. Меры, направленные на обеспечение выполнения ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» обязанностей, предусмотренных законодательством РФ
4. Право субъекта персональных данных на доступ к его персональным данным
5. Правила работы с обезличенными персональными данными в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»

Условия обезличивания

Порядок работы с обезличенными персональными данными

8. Перечень должностей ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

ВВЕДЕНИЕ

1. Настоящий документ «Политика в области обработки и обеспечения безопасности персональных данных в информационных системах персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» (далее - Политика) определяет высокоуровневую политику в отношении обработки в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» персональных данных субъектов и содержит сведения о реализуемых требованиях к защите персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19».
2. Настоящая Политика разработана на основе действующих правовых и нормативных документов по защите конфиденциальной информации и персональных данных.
3. Под персональными данными в настоящем документе понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
4. Настоящая Политика утверждается приказом директора ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» и подлежит пересмотру по мере необходимости.

1. Общие положения

ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» в рамках выполнения своей деятельности осуществляет обработку персональных данных и, в соответствии с действующим

законодательством Российской Федерации, является оператором персональных данных с соответствующими правами и обязанностями, определенными Федеральным законом № 152 от 27.07.2006 «О персональных данных» и иными нормативными правовыми актами Российской Федерации (далее - РФ). Состав обрабатываемых данных, категории субъектов, чьи персональные данные обрабатываются в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», цели и правовые основания их обработки закреплены для каждой информационной системы ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» «Перечнем персональных данных, обрабатываемых в ИСПДн».

Настоящая политика разработана согласно требованию п.2 ч.1 статьи 18.1 Федерального закона от 25.07.2006 № 152-ФЗ «О персональных данных» и подлежит публикации на сайте в разделе «Безопасность персональных данных» в соответствии с требованиями ч.2 статьи 18.1, Федерального закона от 25.07.2006 № 152-ФЗ «О персональных данных».

2. Принципы, правила и цели обработки персональных данных

Обработка персональных данных осуществляется ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;
- обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;
- ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» принимает все необходимые меры по предотвращению разглашения и нарушения конфиденциальности персональных данных;
- при обработке персональных данных обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» принимает необходимые меры по удалению или уточнению неполных или неточных данных;
- хранение персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» осуществляется 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 от

22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» или договором, стороной которого является субъект персональных данных;

- обрабатываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.

Обработка персональных данных осуществляется ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» только в случаях:

- наличия согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством РФ;

- наличия заключенного договора, по которому ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» обязуется осуществлять обработку персональных данных субъектов по поручению оператора;

- необходимости достижения целей, установленных законом для выполнения возложенных на ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» функций, полномочий и обязанностей;

- необходимости осуществления прав и законных интересов ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- предоставления субъектом персональных данных самостоятельно или по его просьбе доступа к его персональным данным для неограниченного количества лиц;

- обработки персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с Федеральным законом;

- организации порядка доступа в помещения ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», в которых производится обработка персональных данных.

Согласно требованиям Федерального закона № 152 от 27.07.2006 «О персональных данных», ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» в установленном порядке прошло регистрацию как оператор персональных данных. В открытом и общедоступном реестре операторов персональных данных, размещенном на официальном сайте Роскомнадзора как уполномоченного лица по защите прав и свобод субъектов персональных данных, содержится следующая актуальная информация:

- адрес ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»;

- цели обработки персональных данных;

- категории персональных данных;

- категории субъектов, персональные данные которых обрабатываются;

- правовое основание обработки персональных данных;

- перечень действий с персональными данными, общее описание используемых ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» способов обработки персональных данных;

- фамилия, имя, отчество физического лица, ответственного в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» за организацию обработки персональных данных, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;

- описание мер, которые ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке

- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии трансграничной передачи персональных данных в процессе их обработки.

ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» обязуется не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ и договором с субъектом.

В соответствии с п.5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утверждённых Постановлением Правительства Российской Федерации от 1 ноября 2012 №1119 ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» обрабатывает специальные, общедоступные и иные категории персональных данных.

На основании Устава в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»:

- не осуществляется трансграничная передача персональных данных;
- не принимается решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы на основании автоматизированной обработки его персональных данных.

3. Меры, направленные на обеспечение выполнения ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» обязанностей, предусмотренных законодательством РФ

ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» осуществляет следующие организационно-технические меры для защиты персональных данных:

- назначение лица, ответственного в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» за организацию обработки персональных данных;
- издание документов, определяющих политику ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ в области информационной безопасности, устранение последствий таких нарушений;
- применение мер по обеспечению безопасности персональных данных в соответствии со статьями 18.1 и 19 Федерального закона № 152 «О персональных данных», включая:
 - определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»;
 - применение мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19».
- осуществление внутреннего контроля соответствия обработки персональных данных законодательству РФ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» в отношении обработки персональных данных, локальным актам ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства РФ, соотношение указанного вреда и принимаемых ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством РФ;
- ознакомление сотрудников ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.
- доступ к содержанию электронного журнала сообщений возможен исключительно для администратора безопасности, или структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационных системах ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19».

4. Право субъекта персональных данных на доступ к его персональным данным

4.1. Субъект персональных данных имеет право на получение сведений, указанных в части 4.6 настоящего раздела, за исключением случаев, предусмотренных законодательством РФ. Субъект персональных данных вправе требовать от лиц, ответственных за обработку персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми

для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.2. Сведения, указанные в части 4.6 настоящего раздела, предоставляются лицами, ответственными за обработку персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», субъекту персональных данных в доступной форме.

4.3. Сведения, указанные в части 4.6 настоящего раздела, предоставляются субъекту персональных данных или его представителю лицами, ответственными за обработку персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», при получении запроса субъекта персональных данных или его представителя в письменной форме.

4.4. В случае, если сведения, указанные в части 4.6 настоящего раздела, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к лицам, ответственным за обработку персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», или направить в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» повторный запрос в письменной форме в целях получения сведений, указанных в части 4.6 настоящего раздела, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

4.5. Субъект персональных данных вправе обратиться повторно к лицам, ответственным за обработку персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», или направить повторный письменный запрос в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» в целях получения сведений, указанных в части 4.6 настоящего раздела, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4.4 настоящего раздела, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

4.6. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» способы обработки персональных данных;
- 4) наименование учреждения и место его нахождения, сведения о лицах (за исключением сотрудников ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» или на основании законодательства РФ;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных законодательством РФ;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», если обработка поручена или будет поручена такому лицу.

5. Правила работы с обезличенными персональными данными В ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19»

УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

5.1 Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от возможности разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19» и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5.2 Способы обезличивания при условии дальнейшей обработки персональных данных:

5.2.1 уменьшение перечня обрабатываемых сведений;

5.2.2 замена части сведений идентификаторами;

5.2.3 обобщение – понижение точности некоторых сведений;

5.2.4 деление сведений на части и обработка в разных информационных системах;

5.2.5 иные способы обезличивания, предусматривающие возможность дальнейшей обработки данных.

5.3 Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

5.4 Для обезличивания персональных данных годятся любые способы, не запрещенные законодательством РФ.

5.6 Решение о необходимости обезличивания персональных данных принимает лицо, ответственное за организацию обработки персональных данных в ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19».

5.7 Ответственные за эксплуатацию ИСПДн готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, если это необходимо.

5.8 Сотрудники структурных подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за эксплуатацию ИСПДн, осуществляют непосредственное обезличивание персональных данных выбранным способом.

ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

5.9 Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

5.10 При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

5.10.1 парольной политики;

5.10.2 антивирусной политики;

5.10.3 правил работы со съемными носителями (если они используются);

5.10.4 правил резервного копирования;

5.10.5 правил доступа в помещения, где расположены элементы информационных систем;

5.11 При обработке обезличенных персональных данных без использования средств автоматизации необходимо выполнение требований п.п. 13, 14, 15 раздела III «Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», утвержденного Постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687:

5.11.1 определение мест хранения персональных данных (материальных носителей);

5.11.2 определение перечня лиц, осуществляющих обработку персональных данных и (или) имеющих к ним доступ;

5.11.3 обеспечение отдельного хранения персональных данных (материальных носителей), обработка которых осуществляется в разных целях;

5.11.4 обеспечение условий хранения персональных данных, гарантирующих их сохранность и исключающих несанкционированный доступ к ним посторонних лиц.

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ СОТРУДНИКОВ ГБУЗ ТО «ОБЛАСТНАЯ БОЛЬНИЦА № 19», ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Главный врач.

2. Заместитель главного врача (ответственный за организацию обработки персональных данных).

3. Руководители структурных подразделений, обрабатывающих ПДн.

4. Системный администратор.