**Положение об обработке персональных данных**

**в муниципальном бюджетном учреждении здравоохранения**

**Городская клиническая поликлиника №5.**

1. Общие положения.

* 1. Настоящее Положение об обработке персональных данных (далее – Положение) в муниципальном бюджетном учреждении здравоохранения Городская клиническая поликлиника № 5 (далее – поликлиника) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
  2. Цель разработки Положения – определение порядка обработки персональных данных в поликлинике, с использованием средств автоматизации и без использования таких средств.
  3. Порядок ввода в действие и изменения Положения:
     1. Настоящее Положение вступает в силу с момента его утверждения главным врачом поликлиники и действует бессрочно, до замены его новым Положением.
     2. Все изменения в Положение вносятся приказом.
  4. Все работники поликлиники, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением.
  5. Режим конфиденциальности персональных данных снимается только в случаях их обезличивания.

1. Основные понятия и состав персональных данных.
   1. Для целей настоящего Положения используются следующие основные понятия:

* информация – сведения (сообщения, данные) независимо от формы их представления;
* персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
* оператор – юридическое (МБУЗ ГКП №5) или физическое лицо (работник поликлиники), 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; субъекты персональных данных – пациенты поликлиники.
* работник – физическое лицо, состоящее в трудовых и (или) иных гражданско-правовых отношениях с МБУЗ ГКП №5 (постоянный сотрудник, совместитель и другие категории работников);
* другие лица – физические лица (субъекты персональных данных), законные представители физических лиц, не относящиеся к категории работников, персональные данные которых обрабатывает поликлиника (уволенные работники, граждане, обращающиеся с заявлениями, жалобами, предложениями; близкие родственники работников, законные представители работников, индивидуальные предприниматели и другие категории субъектов);
* обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
* автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
* распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
* предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
* доступ к информации – возможность получения информации, содержащей персональные данные и ее использования;
* использование персональных данных – действия (операции) с персональными данными, совершаемые поликлиникой в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающие права и свободы субъекта персональных данных или других лиц;
* блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
* 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;
* обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
* общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
* трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
* конфиденциальность персональных данных – обязательное для соблюдения работниками поликлиники, иными получившим доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
* информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
* объект вычислительной техники (ВТ) – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации.

К объектам вычислительной техники относятся автоматизированные системы (АС), автоматизированные рабочие места (АРМ), информационно-вычислительные центры (ИВЦ) и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

* информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
* информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
  1. В состав персональных данных входят сведения, содержащие информацию:

1. Специальные категории данных:

* состояние здоровья;

1. Общедоступные данные:

* Фамилия, Имя, Отчество;
* Адрес;
* Сведения о профессии;

1. Иные категории персональных данных:

* Контактный телефон;
* ИНН;
* Номер свидетельства пенсионного страхования;
* Должность;
* Сведения о доходах;
* Сведения о продвижениях по службе;
* Сведения по инвалидности;
* Данные свидетельства о постановке на налоговый учет;
* Данные о трудовом стаже;
* Данные о вычетах и взносах;
* Количество и возраст детей;
* Сведения о льготах;
* Сведения об образовании, повышении квалификации, аттестации.

3. Сбор, обработка и защита персональных данных.

* 1. Субъект персональных данных предоставляет сотруднику поликлиники достоверные сведения о себе. Сотрудник проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами удостоверяющими личность и иными документами подтверждающие достоверность сведений о субъекте персональных данных.
  2. В соответствии со ст. 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» сотрудники поликлиники при обработке персональных данных должны соблюдать следующие общие требования:
     1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

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

* фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
* наименование и адрес оператора, получающего согласие субъекта персональных данных;
* цель обработки персональных данных;
* перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
* перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
* - срок, в течение которого действует согласие, а также порядок его отзыва.
  + 1. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.
    2. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.
    3. Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.
    4. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.
    5. Защита персональных данных от неправомерного их использования или утраты обеспечивается поликлиникой за счет средств поликлиники в порядке, установленном законодательством.
    6. Отказ гражданина от своих прав на сохранение и защиту тайны недействителен.
  1. Обработка персональных данных субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни разрешается в случаях, если:
* субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных; ? обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
* обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

4. Передача и хранение персональных данных.

* 1. При передаче персональных данных необходимо соблюдать следующие требования:
     1. Не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, установленных федеральным законодательством.
     2. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц письменное подтверждение того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.
     3. Осуществлять передачу персональных данных субъектов в пределах поликлиники в соответствии с настоящим Положением и другими внутренними нормативно – правовыми актами по защите информации.
     4. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.
  2. Персональные данные субъектов могут обрабатываться и храниться, как на бумажных носителях, так и в электронном виде.

1. Уничтожение персональных данных.
   1. Уничтожение документов, содержащих персональные данные, в том числе черновиков, бракованных листов и испорченных копий, должно производиться сотрудниками, выполняющими обработку персональных данных, с последующим составлением акта об уничтожении.
   2. Порядок уничтожения документов, черновиков, испорченных листов, неподписанных проектов документов, содержащих персональные данные:

* документы, черновики документов, испорченные листы, варианты и неподписанные проекты документов разрываются таким образом, чтобы было невозможно дальнейшее восстановление информации. В учетных данных документа (карточке, журнале) делается отметка об уничтожении черновика с указанием количества листов и проставлением подписи сотрудника и даты;
* уничтожение документов, содержащих персональные данные, производится в строгом соответствии со сроками хранения.
  1. Уничтожение персональных данных в электронном виде осуществляется путём удаления информации со всех носителей и резервных копий без возможности дальнейшего восстановления.
  2. Разрешение на уничтожение персональных данных дает главный врач поликлиники.

1. Доступ к персональным данным.
   1. Доступ сотрудников к персональным данным осуществляется на основании разрешительной системы доступа.
   2. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения главного врача поликлиники.
   3. Передача персональных данных третьей стороне возможна только при письменном согласии субъекта персональных данных, либо на основании законодательства Российской Федерации.
2. Правила работы с обезличенными данными.
   1. Обезличиванием персональных данных называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (например, статистические данные).
   2. Обезличивание персональных данных в поликлинике при обработке персональных данных с использованием средств автоматизации осуществляется с помощью специализированного программного обеспечения на основании нормативно правовых актов, правил, инструкций, руководств, регламентов, инструкций на такое программное обеспечение и иных документов для достижения заранее определенных и заявленных целей.
   3. Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации - производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
   4. Работа с обезличенными данными осуществляется в порядке установленным законодательством Российской Федерации и внутренними нормативно-правовыми актами, регулирующими работу с персональными данными.
3. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных.
   1. Доступ сотрудников поликлиники в помещения, в которых ведется обработка персональных данных, осуществляется по Разрешительной системе доступа сотрудников поликлиники в помещения, в которых ведется обработка персональных данных. Разрешительная система доступа готовится и уточняется лицом, ответственным за организацию обработки персональных данных в поликлинике и утверждается главным врачом.
   2. Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется сотрудниками, указанными в Разрешительной системе доступа сотрудников поликлиники в помещения, в которых ведется обработка персональных данных. Пребывание посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии сотрудников, указанных в Разрешительной системе доступа сотрудников поликлиники в помещения, в которых ведется обработка персональных данных.
4. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных.
   1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в поликлинике организуется проведение периодических проверок условий обработки персональных данных. Проверки осуществляются ответственным за организацию обработки персональных данных в поликлинике либо комиссией, образуемой главным врачом поликлиники не реже одного раза в 3 года.
   2. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в поликлинике производится проверка:

* соблюдения принципов обработки персональных данных в поликлинике;
* соответствия локальных актов в области персональных данных поликлиники действующему законодательству Российской Федерации;
* выполнения сотрудниками поликлиники требований и правил (в том числе особых) обработки персональных данных в информационных системах персональных данных поликлиники;
* перечней персональных данных, используемых для решения задач и функций структурными подразделениями поликлиники и необходимости обработки персональных данных в информационных системах персональных данных поликлиники;
* правильность осуществления сбора, систематизации, сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных поликлиники;
* актуальность перечня должностей сотрудников поликлиники, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
* актуальность перечня должностей сотрудников поликлиники, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
* соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных поликлиники;
* соблюдение обязанностей поликлиники, предусмотренных действующим законодательством в области персональных данных;
* порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных поликлиники, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;
* наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных поликлиники;
* актуальность сведений, содержащихся в уведомлении поликлиники об обработке персональных данных;
* актуальность перечня информационных систем персональных данных в поликлинике;
* наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных, для каждой информационной системы персональных данных поликлиники;
* знания и соблюдение сотрудниками поликлиники положений действующего законодательства Российской Федерации в области персональных данных;
* знания и соблюдение сотрудниками поликлиники положений локальных актов поликлиники в области обработки и обеспечения безопасности персональных данных;
* знания и соблюдение сотрудниками поликлиники инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
* соблюдение сотрудниками поликлиники конфиденциальности персональных данных;
* актуальность локальных актов поликлиники в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;
* соблюдение сотрудниками поликлиники требований по обеспечению безопасности персональных данных;
* наличие локальных актов поликлиники, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных поликлиники;
* иных вопросов.
  1. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю поликлиники докладывает ответственный за организацию обработки персональных данных, либо председатель комиссии.

1. Права субъекта персональных данных.
   1. Субъект персональных данных имеет право получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей его персональные данные.
   2. Субъект персональных данных имеет право требовать от сотрудников поликлиники уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для работы поликлиники персональных данных.
   3. Субъект персональных данных имеет право получать информацию, которая касается обработки его персональных данных, в том числе содержащей:

* подтверждение факта обработки персональных данных;
* правовые основания и цели обработки персональных данных;
* цели и применяемые способы обработки персональных данных;
* наименование и место нахождения поликлиники, сведения о лицах (за исключением работников поликлиники), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
* обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
* сроки обработки персональных данных, в том числе сроки их хранения;
* порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
* информацию об осуществленной или о предполагаемой трансграничной передаче данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.
  1. Субъект персональных данных имеет право требовать извещения сотрудниками поликлиники всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

1. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

Работники поликлиники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.