

УТВЕРЖДЕНЫ
приказом ГБУЗ НСО «ДГКСП»
от 18 ноября 2016 года № 220

Правила обработки персональных данных в Государственном бюджетном учреждении здравоохранения Новосибирской области "Детская городская клиническая стоматологическая поликлиника", устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

I. Общие положения

1.1. Настоящими Правилами обработки персональных данных в Государственном бюджетном учреждении здравоохранения Новосибирской области "Детская городская клиническая стоматологическая поликлиника" (далее - ГБУЗ НСО «ДГКСП»), устанавливающими процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющими для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (далее - Правила) определяются цели, содержание и порядок обработки персональных данных, меры по обеспечению безопасности персональных данных при их обработке в ГБУЗ НСО «ДГКСП», а также устанавливаются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных. Настоящие Правила определяют политику ГБУЗ НСО «ДГКСП» как оператора, осуществляющего обработку персональных данных. Настоящие Правила разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее - Федеральный закон "О персональных данных"), постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", постановления Правительства Российской Федерации от 21 марта 2012 года № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами", 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" (далее - постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119). Правовой основой настоящих Правил также являются Трудовой кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральный закон от 25 декабря 2008 года № 273-ФЗ "О противодействии коррупции", Федеральный закон от 2 мая 2006 года № 59-ФЗ "О порядке рассмотрения обращений

граждан Российской Федерации", Федеральный закон от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», Приказ департамента здравоохранения Новосибирской области от 16.05.2008 № 508 «О мерах по защите информации конфиденциального характера».

1.2. Действие настоящих Правил не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с Федеральным законом от 22 октября 2004 года № 125-ФЗ "Об архивном деле в Российской Федерации"; обработке персональных данных, отнесенных в порядке, установленном Законом Российской Федерации от 21 июля 1993 года № 5485-1 "О государственной тайне", к сведениям, составляющим государственную тайну.

II. Условия обработки персональных данных

2.1. Настоящими Правилами определяются следующие цели обработки персональных данных, относительно субъектов персональных данных.

2.1.1. Персональные данные работников ГБУЗ НСО «ДГКСП», состоящих с ГБУЗ НСО «ДГКСП» в трудовых отношениях, обрабатываются в целях обеспечения кадровой работы, в том числе в целях содействия работникам ГБУЗ НСО «ДГКСП» в выполнении работы, обучении и должностном росте, учета результатов исполнения работниками ГБУЗ НСО «ДГКСП» должностных обязанностей, обеспечения работнику ГБУЗ НСО «ДГКСП» установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности принадлежащего ему имущества и имущества ГБУЗ НСО «ДГКСП», а также в целях противодействия коррупции.

2.1.2. Персональные данные физических лиц, обратившихся в ГБУЗ НСО «ДГКСП» в письменной форме или в форме электронного документа, а также с устным обращением, обрабатываются в целях их рассмотрения и последующего уведомления о результатах рассмотрения.

2.1.3. Персональные данные лиц, обратившихся в ГБУЗ НСО «ДГКСП» для оказания медицинских услуг. Персональные данные указанных лиц также могут обрабатываться в целях предоставления государственных услуг и осуществления государственных функций в электронном виде.

2.1.4. Персональные данные различных субъектов персональных данных могут обрабатываться в иных целях, указанных в письменном согласии субъекта персональных данных на обработку его персональных данных.

2.2. Согласие на обработку персональных данных субъекта персональных данных, чьи данные обрабатываются в целях, указанных в пункте 2.1.1 настоящих Правил, не требуется при обработке персональных данных в соответствующих целях на основании Трудового кодекса Российской Федерации.

2.2.3. Необходимо получить согласие субъекта персональных данных на обработку его персональных данных:

– при передаче персональных данных третьей стороне (за исключением случаев, предусмотренных федеральными законами);

– при распространении (в том числе при размещении на официальном сайте ГБУЗ НСО «ДГКСП») персональных данных.

2.2.4. Согласие на обработку персональных данных субъекта необходимо получать непосредственно у субъекта персональных данных в любой форме, позволяющей подтвердить факт его получения, если иное не установлено федеральными законами.

2.2.5. Организация сбора и хранения письменных согласий на обработку персональных данных субъектов персональных данных возлагается на отделения ГБУЗ НСО «ДГКСП», непосредственно осуществляющие обработку персональных данных.

III. Действия (операции), совершаемые с персональными данными

3.1. ГБУЗ НСО «ДГКСП» осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

3.1.1. Сбор, запись, систематизация, накопление и уточнение персональных данных, обрабатываемых в случаях, предусмотренных пунктом 2.1.1 настоящих Правил, осуществляется путем:

- копирования оригиналов документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях);
- получения оригиналов необходимых документов (трудовая книжка, автобиография, иные документы, предоставляемые в кадровое подразделение ГБУЗ НСО «ДГКСП»);
- создания персональных данных в ходе кадровой работы;
- внесения сведений в Единую Государственную Информационную Систему в сфере здравоохранения Новосибирской области (далее - ЕГИСЗ НСО);
- внесения сведений в информационные системы не являющиеся подсистемами ЕГИСЗ НСО.

3.1.2. Сбор, запись, систематизация, накопление и уточнение персональных данных, обрабатываемых в целях, указанных в пункте 2.1.2 настоящих Правил, осуществляется путем:

- получения письменных обращений в установленной форме;
- регистрации персональных данных на бумажных и электронных носителях информации.

3.1.3. Сбор, запись, систематизация, накопление и уточнение персональных данных, обрабатываемых в случаях, предусмотренных пунктом 2.1.3 настоящих Правил, осуществляется путем:

- получения необходимой информации (в том числе в документированном виде) непосредственно от обратившихся в ГБУЗ НСО «ДГКСП»;
- получения объяснений, информации, справок от физических лиц, организаций и органов, находящихся на территории Российской Федерации, а также на территориях иностранных государств, в порядке, установленном международным договором Российской Федерации;
- фиксации (регистрации) в соответствующих журналах, книгах;
- создания персональных данных в ходе оказания медицинских услуг;
- внесения сведений в подсистемы ЕГИСЗ НСО, а также в информационные системы персональных данных, не являющиеся подсистемами ЕГИСЗ НСО.

3.1.4. Сбор, запись, систематизация, накопление и уточнение персональных данных, обрабатываемых в случаях, предусмотренных пунктом 2.1.4 настоящих Правил, осуществляется путем получения персональных данных непосредственно от субъектов персональных данных, давших свое согласие на их обработку, или иным образом, указанным в письменном согласии.

3.2. При сборе персональных данных в случаях, предусмотренных пунктами 2.1.1-2.1.3 настоящих Правил, работник ГБУЗ НСО «ДГКСП», осуществляющий получение персональных данных непосредственно от субъекта персональных данных, обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3.3. Предоставление и распространение персональных данных осуществляется в соответствии с федеральными законами, на основании которых они обрабатываются, в порядке, предусмотренном главой 7 настоящих Правил.

3.5. Использование персональных данных осуществляется в соответствии с федеральными законами, на основании которых они обрабатываются. Возможность использовать персональные данные имеют исключительно работники, допущенные к персональным данным в порядке, предусмотренном главой 7 настоящих Правил.

3.6. В зависимости от конкретной цели обработки персональных данных, обрабатываемых в случаях, предусмотренных пунктами 2.1.1-2.1.3 настоящих Правил, ГБУЗ НСО «ДГКСП» также могут совершаться иные действия, предусмотренные федеральными законами, на основании которых они обрабатываются.

IV. Лица, ответственные за организацию обработки персональных данных

4.1. Лицо, ответственное за организацию обработки персональных данных, получает письменные указания непосредственно от руководителя ГБУЗ НСО «ДГКСП»

V. Организация хранения персональных данных

5.1. Персональные данные хранятся на бумажном носителе в отделениях ГБУЗ НСО «ДГКСП», в функции которых входит обработка персональных данных. Персональные данные хранятся в электронном виде в подсистемах ЕГИСЗ НСО и в информационных системах персональных данных ГБУЗ НСО «ДГКСП», не являющихся подсистемами ЕГИСЗ НСО.

5.2. Сроки хранения персональных данных на бумажном носителе определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

5.3. Срок хранения персональных данных в электронном виде должен соответствовать сроку хранения бумажных носителей.

5.4. При хранении персональных данных на электронных носителях работником ГБУЗ НСО «ДГКСП» (по информатизации) обеспечивается регулярное резервное копирование информации с целью недопущения потери персональных данных при выходе из строя носителей персональных данных.

5.5. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящими Правилами, без использования средств вычислительной техники (без использования средств автоматизации).

5.6. Руководителем отделения ГБУЗ НСО «ДГКСП», осуществляющего обработку персональных данных, устанавливается контроль за хранением и использованием носителей персональных данных, не допускающий несанкционированного использования, уточнения, распространения и уничтожения персональных данных, находящихся на этих носителях.

5.7. Уточнение (изменение, дополнение) персональных данных при осуществлении их обработки без использования средств вычислительной техники (без использования средств автоматизации) может производиться путем обновления (в том числе частичного) или изменения данных на материальном носителе. Если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном

носителе сведений об изменениях, вносимых в персональные данные, либо путем изготовления нового материального носителя с уточненными персональными данными.

5.8. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

5.9. Вывод на печать документов, содержащих персональные данные, допускается в связи с исполнением служебных обязанностей, в том числе в целях передачи печатных копий субъектам персональных данных либо лицам, допущенным в соответствии с пунктом 6.1 настоящими Правилами к работе с персональными данными.

VI. Допуск работников ГБУЗ НСО «ДГКСП» к работе с персональными данными

6.1. К работе с персональными данными допускаются работники, замещающие должности врачей, среднего медицинского персонала и административно-управленческого персонала.

6.2. При реализации работником ГБУЗ НСО «ДГКСП» прав субъекта персональных данных его персональные данные должны предоставляться ему таким образом, чтобы не нарушалась конфиденциальность персональных данных других субъектов персональных данных.

6.3. Требования по соблюдению конфиденциальности персональных данных являются обязательными при допуске работника ГБУЗ НСО «ДГКСП» к работе с персональными данными. Работник, получивший доступ к персональным данным, обязан не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами. Работник, допущенный к обработке персональных данных, принимает на себя обязательства в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей. Обязательство в письменной форме приобщается к личному делу работника.

6.4. Работники, допущенные к обработке персональных данных, должны быть проинформированы о характере обработки, категориях обрабатываемых персональных данных, а также об особенностях и условиях осуществления такой обработки, установленных настоящими Правилами.

6.5. При осуществлении доступа к персональным данным, обрабатываемым в подсистемах ЕГИСЗ НСО и информационных системах персональных данных ГБУЗ НСО «ДГКСП», не являющихся подсистемами ЕГИСЗ НСО, должна применяться система разграничения прав доступа, на основе утверждаемых приказом ГБУЗ НСО «ДГКСП» правил разграничения доступа к информации, обрабатываемой в информационной системе. Правила разграничения доступа согласовываются с лицом, ответственным за организацию обработки персональных данных в ГБУЗ НСО «ДГКСП».

6.6. Об инцидентах, связанных с попытками нарушения правил разграничения доступа и несанкционированным доступом, докладывается лицу, ответственному за организацию обработки персональных данных в ГБУЗ НСО «ДГКСП». Срок хранения регистрационной информации должен составлять не менее 10 дней.

VII. Порядок предоставления персональных данных

7.1. Не допускается предоставление баз, банков данных, списков, содержащих персональные данные, государственному органу, его территориальному органу, органу местного самоуправления или организации, подведомственной государственному органу,

органу местного самоуправления, а также физическому или юридическому лицу, за исключением случаев, предусмотренных федеральными законами.

7.2. ГБУЗ НСО «ДГКСП» в соответствии со статьей 6 Федерального закона "О персональных данных" может поручать обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральными законами, на основании договора. В соответствующем договоре указываются порядок предоставления персональных данных, обязательства сторон по соблюдению конфиденциальности, цель обработки, ограничение на использование персональных данных, а также требования к защите обрабатываемых персональных данных. При этом условием поручения обработки является наличие организации в реестре операторов персональных данных.

7.3. ГБУЗ НСО «ДГКСП» может поручать защиту персональных данных организации на основании договора, в котором указываются порядок предоставления персональных данных, обязательства сторон по соблюдению конфиденциальности и ограничения на использование персональных данных, а также требования к защите обрабатываемых персональных данных. При этом условием поручения защиты является наличие у организации лицензии на осуществление деятельности по технической защите конфиденциальной информации.

7.4. ГБУЗ НСО «ДГКСП» передает персональные данные субъекта персональных данных государственному органу, его территориальному органу, органу местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физическому или юридическому лицу на основании запроса о предоставлении персональных данных (далее - запрос).

7.5. Запрос оформляется в письменном виде на бланках в соответствии с требованиями, установленными Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти, и направляется фельдсвязью, почтовым отправлением, с нарочным или в форме электронного документа.

7.6. Запрос должен быть подписан уполномоченным должностным лицом, содержать указание цели и правовые основания для затребования персональных данных и срок предоставления этой информации, если иное не установлено федеральными законами.

7.7. При направлении запроса по информационно-телекоммуникационным сетям стандарт, формат и процедуру информационного взаимодействия с контрагентом определяет ГБУЗ НСО «ДГКСП» в соответствии с действующим законодательством. Подпись должностного лица подтверждается квалифицированной электронной подписью.

7.8. Запрос физического лица о предоставлении его персональных данных, в соответствии со статьей 14 Федерального закона "О персональных данных", должен содержать реквизиты документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения, подтверждающие участие субъекта персональных данных в отношениях с ГБУЗ НСО «ДГКСП», либо сведения, иным образом подтверждающие факт обработки персональных данных ГБУЗ НСО «ДГКСП», подпись субъекта персональных данных или его представителя.

7.9. Запрос подлежит рассмотрению ГБУЗ НСО «ДГКСП», если в нем указывается положение федерального закона, устанавливающего право обратившегося государственного органа, его территориального органа, органа местного самоуправления или организации, подведомственной государственному органу, органу местного самоуправления, а также физического или юридического лица на получение запрашиваемых персональных данных или в случае заключения договора (соглашения) об информационном взаимодействии с ГБУЗ НСО «ДГКСП».

7.10. Обоснованием (мотивом) запроса является конкретная цель, связанная с реализацией гражданином своих прав или исполнением определенных федеральным

законом обязанностей, для достижения которых ему необходимо использовать запрашиваемые персональные данные. Запросы, по форме и содержанию не отвечающие требованиям пункта 7.9 настоящих Правил, исполнению не подлежат.

7.11. Предоставление гражданам информации, содержащей персональные данные, посредством информационно-телекоммуникационной сети в электронном виде в форме электронного документа, подписанного электронной подписью, осуществляется в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг".

VIII. Требования к защите персональных данных при их обработке без использования средств вычислительной техники

8.1. Обработка персональных данных без использования средств вычислительной техники (без использования средств автоматизации) осуществляется работниками ГБУЗ НСО «ДГКСП».

8.2. Печатная копия документа, созданная в целях передачи определенному субъекту персональных данных, не должна содержать персональные данные других субъектов персональных данных, за исключением случаев, определенных действующим законодательством.

8.3. Запрещается использовать печатные копии документов, содержащих персональные данные, для повторной печати (в качестве черновиков).

8.4. Типовые формы документов, характер информации в которых предполагает или допускает включение в них персональных данных, утверждаются ГБУЗ НСО «ДГКСП» с соблюдением условий, предусмотренных пунктом 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

IX. Требования к защите персональных данных при их обработке в информационных системах персональных данных

9.1. Безопасность персональных данных при их обработке в информационных системах персональных данных ГБУЗ НСО «ДГКСП», как являющихся, так и не являющихся подсистемами ЕГИСЗ НСО, обеспечивается при помощи системы защиты персональных данных, нейтрализующей актуальные угрозы безопасности персональных данных.

9.2. Меры по обеспечению безопасности персональных данных должны обеспечить надлежащий уровень безопасности с учетом соразмерности затрат на их реализацию и опасности угроз, обусловленных природой защищаемых данных и условиями их обработки.

9.3. В целях определения угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении функций, возложенных на ГБУЗ НСО «ДГКСП», ГБУЗ НСО «ДГКСП» ведет и поддерживает в актуальном состоянии техническую документацию на информационные системы персональных данных.

9.4. ГБУЗ НСО «ДГКСП» в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 принимает организационные меры, необходимые для определения уровня защищенности персональных данных для информационных систем персональных данных, и выполнения требований к защите персональных данных при их обработке в информационных системах персональных

данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

9.5. Выбор организационных и технических мер по защите персональных данных в информационных системах ГБУЗ НСО «ДГКСП» осуществляется в соответствии с приказом ФСБ России от 10 июля 2014 года № 378 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" и приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

9.6. Средства защиты информации, применяемые для реализации выбранных методов и способов защиты информации, в порядке, установленном законодательством о техническом регулировании, проходят процедуру оценки соответствия.

9.7. При обработке персональных данных в информационных системах персональных данных должна проводиться оценка эффективности принимаемых мер по обеспечению безопасности персональных данных, а также выполняться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

9.8. До ввода в промышленную эксплуатацию информационной системы персональных данных ГБУЗ НСО «ДГКСП», организуются мероприятия по оценке и дается заключение об эффективности принимаемых мер по обеспечению безопасности персональных данных. В дальнейшем оценка эффективности проводится в рамках внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

9.9. Администратор информационной безопасности ГБУЗ НСО «ДГКСП» осуществляет выявление и фиксацию фактов несанкционированного доступа к персональным данным, а также принимает меры по проверке и расследованию нарушений (инцидентов) информационной безопасности, в том числе с использованием программных, программно-аппаратных и технических средств.

9.10. Администратор информационной системы персональных данных осуществляющий сопровождение информационных систем в ГБУЗ НСО «ДГКСП», обеспечивает восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Х. Заключительные положения

10.1. При создании новых баз данных, реестров, таблиц, анкет, книг, журналов, предусматривающих занесение в них персональных данных, их использование согласовывается с лицом, ответственным за организацию обработки персональных данных в ГБУЗ НСО «ДГКСП».

10.2. При внедрении новых информационных систем персональных данных, изменении объема (содержания), порядка и целей обработки персональных данных лицо, ответственное за организацию обработки персональных данных в ГБУЗ НСО «ДГКСП», инициирует внесение изменений в уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных в ГБУЗ НСО «ДГКСП».

10.3. Руководители отделений ГБУЗ НСО «ДГКСП», в которых обрабатываются персональные данные, осуществляют контроль за соблюдением правил разграничения доступа к персональным данным и требований по обеспечению конфиденциальности персональных данных в рамках своих полномочий.

10.4. Работники ГБУЗ НСО «ДГКСП», допущенные в установленном порядке к обработке персональных данных, несут персональную ответственность за нарушение требований по обработке персональных данных в соответствии со статьей 24 Федерального закона "О персональных данных".

10.5. Контроль за выполнением предусмотренных мер защиты персональных данных возлагается на лицо, ответственное за организацию обработки персональных данных в ГБУЗ НСО «ДГКСП».