Приложение № 1
к приказу ОБУЗ «КГДП»
от «23» марта 2023 г. № 149

П О Л И Т И К А

обработки персональных данных в областном бюджетном учреждении здравоохранения «Курская городская детская поликлиника»

I. Общие положения

1.1. Настоящая Политика обработки персональных данных в областном бюджетном учреждении здравоохранения «Курская городская детская поликлиника» комитета здравоохранения Курской области (далее – Политика) подготовлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных» и является основополагающим внутренним регулятивным документом (локальным правовым актом) областного бюджетного учреждения здравоохранения «Курская городская детская поликлиника» комитета здравоохранения Курской области (далее – Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной, врачебной и других охраняемых законом тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до её утверждения.

1.4. Обработка ПДн в Организации осуществляется в связи с выполнением Организацией функций, предусмотренных её учредительными документами, и определяемых:

- Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных»;
- постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными действующими нормативными правовыми актами РФ.

Кроме того, обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя, в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Политика подлежит изменению, дополнению в следующих случаях:

- при изменении законодательства Российской Федерации в области обработки и защиты ПДн;
- при изменении целей обработки ПДн, структуры информационных и/или телекоммуникационных систем (или введении новых);
- при применении новых технологий обработки ПДн;
- при появлении необходимости в изменении процесса обработки ПДн, связанной с деятельностью Организации;
- по результатам контроля выполнения требований по обработке и защите ПДн;
- - по решению руководства Организации, но в любом случае не реже одного раза в пять лет.

Изменения и дополнения в Политику вносятся приказами Организации.

При внесении изменений в заголовке Политики указывается дата последнего обновления редакции.

Новая редакция Политики вступает в силу с даты, указанной в соответствующем приказе Организации.

Каждая новая редакция Политики должна быть опубликована на сайте ОБУЗ «КГДП» http://www.muzdp8.ru. в установленный законом срок.

1.6. Действующая редакция хранится в месте нахождения Организации по адресу: г. Курск, пр. Энтузиастов, д.18, электронная версия Политики – на сайте по адресу: http://www.muzdp8.ru.

1.7. Сведения об Организации (Операторе):

- Наименование Оператора – Областное бюджетное учреждение здравоохранения «Курская городская детская поликлиника»;
- Адрес местонахождения: 305048, г. Курск, проспект Энтузиастов, 18;
- тел.: 8 (4712) 52-54-49;
- e-mail: kgdp@sovtest.ru
- ИНН 4629040100
- Регистрационный номер записи в Реестре операторов, осуществляющих обработку персональных данных: 10-0096658.

II. Термины и принятые сокращения

- **персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- **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.
- **оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
- **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.
- **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу 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;
- **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;
- **информационная система персональных данных (ИСПД)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- **персональные данные, разрешённые субъектом персональных данных для распространения** – персональные данные, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных путём дачи согласия на обработку персональных данных, разрешённых субъектом

персональных данных для распространения в порядке, предусмотренном законом.

III. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

- **законность:** защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;
- **системность:** обработка ПДн в Организации осуществляется с учётом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
- **комплексность:** защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;
- **непрерывность:** защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- **своевременность:** меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- **преемственность и непрерывность совершенствования:** модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учётом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- **персональная ответственность:** ответственность за обеспечение безопасности ПДн возлагается на работников в пределах их должностных обязанностей, связанных с обработкой и защитой ПДн;
- **минимизация прав доступа:** доступ к ПДн предоставляется работникам только в объёме, необходимом для выполнения их должностных обязанностей;
- **гибкость:** обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объёма и состава обрабатываемых ПДн;

- **специализация и профессионализм:** реализация мер по обеспечению безопасности ПДн осуществляются работниками, имеющими необходимые для этого квалификацию и опыт;
- **эффективность процедур отбора кадров:** кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
- **наблюдаемость и прозрачность:** меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- **непрерывность контроля и оценки:** устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожатся или обезличиваются.

3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

IV. Обработка персональных данных

4.1. Получение ПДн.

4.1.1. Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлён об этом или от него должно быть получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение

4.1.3. Документы, содержащие ПДн создаются путём:

- копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
- внесения сведений в учётные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами (локальными правовыми актами) Организации.

4.2. Обработка ПДн

4.2.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных на оператора законодательством Российской Федерации функций, полномочий и обязанностей.

Доступ работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов (локальных правовых актов) Организации.

Допущенные к обработке ПДн работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

4.2.2. Цели обработки ПДн:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения задач и функций, определённых Уставом Организации, в соответствии с Федеральными законами от «Об основах охраны здоровья граждан Российской Федерации» 21.11.2011 г. № 323-ФЗ, «Об обязательном медицинском страховании граждан в Российской Федерации» от 29.11.2010 г. № 326-ФЗ, иными действующими нормативными правовыми актами;
- осуществление трудовых отношений, включая исполнение обязанностей, возложенных законодательством на Организацию, в т.ч. связанных с представлением персональных данных в налоговые органы, Социальный фонд Российской Федерации, Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы и исполнением судебных актов, актов других государственных органов или должностных лиц;
- участие в закупках в рамках контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных нужд, осуществление гражданско-правовых отношений, а также реализация прав и законных интересов Организации в рамках ведения видов деятельности, предусмотренных Уставом.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с Организацией в трудовых отношениях;
- физические лица, являющие близкими родственниками работников Организации;
- физические лица, уволившиеся из Организации;

- физические лица, являющиеся кандидатами при приёме на работу в Организацию;
- физические лица, представляющие интересы контрагентов Организации в закупках в рамках контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных нужд, лиц, состоящих с Организацией в гражданско-правовых и прочих договорных отношениях;
- физические лица, обратившиеся в Организацию за медицинской помощью.

4.2.4. ПДн, обрабатываемые Организацией:

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов при приёме на работу в Организацию;
- данные, полученные при участии в закупках в рамках контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных нужд, осуществлении гражданско-правовых отношений, а также реализации прав и законных интересов Организации в рамках ведения видов деятельности, предусмотренных Уставом;
- данные, полученные при оказании медицинской помощи.

Полный список ПДн представлен в Перечне ПДн, утверждённом главным врачом Организации.

4.2.5. Обработка персональных данных ведётся:

- с использованием средств автоматизации.
- без использования средств автоматизации.

4.3. Хранение ПДн

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

4.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение ПДн

4.4.1. Уничтожение документов (носителей), содержащих ПДн производится путём сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.2. ПДн на электронных носителях уничтожаются путём стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

4.5. Передача ПДн

4.5.1. Организация передаёт ПДн третьим лицам в следующих случаях:

- субъект выразил своё согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

- Социальный фонд РФ для учёта (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;

V. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с работниками, партнёрами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

5.5. Основными мерами защиты ПДн, используемыми Организацией, являются:

5.5.1. Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний

контроль за соблюдением учреждением и его работниками требований к защите ПДн;

5.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;

5.5.3. Разработка политики в отношении обработки персональных данных;

5.5.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учёта всех действий, совершаемых с ПДн в ИСПД;

5.5.5. Установление индивидуальных паролей доступа работников в информационную систему в соответствии с их производственными обязанностями;

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учёт машинных носителей ПДн, обеспечение их сохранности;

5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

5.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

5.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;

5.5.10. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн

5.5.11. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учёта действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

5.5.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5.5.13. Обучение работников Организации непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

5.5.14. Осуществление внутреннего контроля и аудита.

VI. Основные права субъекта ПДн и обязанности Организации

6.1. Основные права субъекта ПДн

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

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;

- цели и применяемые оператором 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;
- 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 законодательством о персональных 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 настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн вправе требовать от оператора 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.

Субъект персональных данных вправе по своему усмотрению определять те персональные данные в каждой категории персональных данных, доступ к которым для распространения неограниченному кругу лиц он предоставляет Организации, а к каким запрещает, путём дачи письменного согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения в порядке, предусмотренном законом.

6.2. Обязанности Организации

Организация обязана:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта об этом;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;

- давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн;
- запросить у субъекта ПДн согласие на обработку персональных данных, разрешённых им по своему усмотрению для распространения неограниченному кругу лиц в порядке, предусмотренном законом, при этом организация не вправе каким-либо образом ограничивать свободу выбора этих ПДн субъектом ПДн.

VII. Заключительные положения

7.1. Ответственность работников Организации, осуществляющих обработку персональных данных и имеющих право доступа к ним, за невыполнение (ненадлежащее выполнение) положений Политики, а также требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с действующим законодательством Российской Федерации и локальными правовыми актами Организации.

7.2. Ответственным за организацию обработки и обеспечения безопасности персональных данных назначен заместитель главного врача по информационной безопасности Барышников В.Н., тел.: (4712) 52-54-47

7.3. Уполномоченный орган по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Адрес местонахождения: 109992, г. Москва, Китайгородский пр., д.7, стр.2.

Официальный сайт – https://rkn.gov.ru

Общий электронный адрес Роскомнадзора – rsoc_in@rkn.gov.ru

Справочно-информационный центр:

- (495) 983-33-93 (тел);
- (495) 587-44-68 (факс)

Уполномоченный орган по защите прав субъектов персональных данных в Курской области - Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Курской области (Управление Роскомнадзора по Курской области)

Адрес местонахождения: 305000, г. Курск, Красная площадь, д.8, 1 эт.

e-mail: rsockanc46@rkn.gov.ru, rsoc46@rkn.gov.ru

Официальный сайт – https://46.rkn.gov.ru

Телефон приёмной (справочная, факс): (4712) 34-94-93

Отдел по защите прав субъектов персональных данных: (4712) 34-94-99