«Утверждаю»
Главный врач ГБУЗ «ОКБ»
_____ С.Е. Козлов
«19» октября 2020 года

Политика
в отношении обработки и защиты персональных данных
Государственного бюджетного учреждения здравоохранения Тверской области
«Областная клиническая больница»

1. Общие положения

1.1. Настоящий документ составлен в соответствии с п. 1-2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом ГБУЗ «ОКБ» (далее – Учреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПДн).

1.2. Политика в отношении обработки и защиты персональных данных (далее – 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 Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайны.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Учреждением 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 ее утверждения.

1.4. Учреждение имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента издания приказа по Учреждению, которым утверждена Политика, если иное не предусмотрено новой редакцией Политики. Утвержденная Политика размещается на сайте Учреждения.

1.5. Действующая редакция хранится в месте нахождения Учреждения по адресу: Тверская область, г. Тверь, Петербургское шоссе, д. 105, электронная версия Политики – на сайте по адресу: http://окб-тверь.рф.

2. Правовое основание обработки персональных данных

Обработка ПДн в Учреждении осуществляется на основании:

- Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федерального закона от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федерального закона от 20 июля 2012 г. № 125-ФЗ «О донорстве крови и ее компонентов»;
- Федерального закона от 16 июля 1999 г. № 165-ФЗ «Об основах обязательного социального страхования»;
- Федерального закона от 29 декабря 2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- Федерального закона от 30 декабря 2001 г. № 197-ФЗ «Трудовой кодекс РФ»;
- Федерального закона от 31 июля 1998 г. № 146-ФЗ «Налоговый кодекс РФ»;
- Федерального закона от 30 ноября 1994 г. № 51-ФЗ «Гражданский кодекс РФ»;
- Федерального закона от 15 декабря 2001 г. № 167-ФЗ «Об обязательном пенсионном страховании»;
- Федерального закона от 01 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учёте в системе обязательного пенсионного страхования»;
- Федерального закона от 06 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете»;
- Федерального закона от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации;
- Федерального закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федерального закона от 09 января 1996 г. № 3-ФЗ «О радиационной безопасности населения»;
- Федерального закона от 08 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах»;
- Федерального закона от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств»;
- Федерального закона от 28 марта 1998 г. № 53-ФЗ «О воинской обязанности и военной службе»;
- Постановления Правительства РФ от 16 апреля 2003 г. № 225 «О трудовых книжках»;

- Постановления Правительства РФ от 04 октября 2012 г. № 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;
- Постановления Правительства РФ от 06 августа 1998 г. № 892 "Об утверждении Правил допуска лиц к работе с наркотическими средствами и психотропными веществами, а также к деятельности, связанной с оборотом прекурсоров наркотических средств и психотропных веществ";
- Постановления Правительства РФ от 27 ноября 2006 г. № 719 «Об утверждении положения о воинском учете»;
- Национального стандарта РФ «Электронная история болезни» ГОСТ Р 52636-2006, утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 407-ст;
- Приказа Минздрава СССР от 04 октября 1980 г. № 1030 «Об утверждении форм первичной медицинской документации учреждений здравоохранения» в соответствии с Письмом Минздравсоцразвития РФ от 30 ноября 2009 г. N 14-6/242888;
- иных федеральных законов, указы и распоряжений Президента РФ, постановлений и распоряжений Правительства РФ, нормативных правовых актов федеральных органов исполнительной власти, в частности, Минздрава России, Минздравсоцразвития России в сфере здравоохранения, а также иные нормативные документы, регламентирующие справочную и информационную работу медицинских учреждений и организаций;
- согласия субъекта персональных данных на обработку его персональных данных.

3. 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 неопределенному 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 (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

4. Принципы обеспечения безопасности персональных данных

4.1. Основной задачей обеспечения безопасности ПДн при их обработке в Учреждении 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.

4.2. Для обеспечения безопасности ПДн Учреждение 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 Учреждении осуществляется с учетом 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 Учреждения и других имеющихся в Учреждении 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 Учреждении с учетом 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 обязанностей, связанных с обработкой и защитой ПДн;
- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования ИСПДн Учреждения, а также объема 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 Учреждения 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.

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

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

5. Обработка персональных данных

5.1. Получение ПДн

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

5.1.2. 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.

5.1.3. Документы, содержащие ПДн, создаются путем:

а. копирования (сканирования) оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б. внесения сведений в учетные формы;

в. получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Учреждением, определяется в соответствии с законодательством РФ, а также внутренними регулятивными документами Учреждения.

5.2. Обработка ПДн

5.2.1. **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 законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных

либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами Учреждения, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

Учреждением производится устранение выявленных нарушений требований законодательства об обработке и защите ПДн.

5.2.2. **Цели обработки ПДн:**

- обеспечение Учреждением оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011г № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

5.2.3. **Категории субъектов персональных данных**

В Учреждении обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- контрагенты;
- физические лица, обратившиеся в учреждение за медицинской помощью;
- физические лица, являющиеся родственниками пациентов;
- посетители пациентов;
- доноры;
- пользователи библиотеки (читатели);
- студенты, проходящие практику;

– граждане, оставившие обращение в ГБУЗ "ОКБ";

– посетители сайта

5.2.4. **Категории ПДн, обрабатываемые Учреждением:**

– специальные категории персональных данных;

– иные категории персональных данных;

Полный список ПДн представлен в Перечне ПДн, утвержденном главным врачом Учреждения.

5.2.5. **Обработка персональных данных ведется:**

– с использованием средств автоматизации;

– без использования средств автоматизации;

– смешанная обработка.

5.3. Хранение ПДн

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

5.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах (ящиках, сейфах), либо в запираемых помещениях с ограниченным правом доступа.

5.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных базах данных.

5.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПДн.

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

5.4. Уничтожение ПДн

5.4.1. Уничтожение материальных носителей ПДн (бумажных документов, жестких дисков и т.д.), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Также допускается заключение договора на уничтожение со сторонними организациями, при условии соблюдения режима конфиденциальности.

5.4.2. Уничтожение ПДн, записанных на электронные носители, без непосредственного уничтожения самого носителя, производится способом, в результате которого невозможно восстановить содержание ПДн в ИСПДн.

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

5.5. Передача ПДн

5.5.1. Учреждение передает ПДн третьим лицам в следующих случаях:

- субъект выразил свое согласие на передачу своих ПДн;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

5.5.2. Перечень лиц, которым передаются ПДн:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (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 и согласия субъекта);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- бюро кредитных историй (с согласия субъекта);
- юридические фирмы, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта);
- Министерство здравоохранения Тверской области (с согласия субъекта);
- Главное управление Региональной безопасности Тверской области (с согласия субъекта).

6. Защита персональных данных

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

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

6.3. Подсистема организационной защиты включает в себя меры административного и процедурного характера, регламентирующие процессы функционирования системы

обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

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

6.5. Основными мерами защиты ПДн, используемыми Учреждением, являются:

6.5.1. Назначение лиц, ответственных за организацию обработки ПДн, которые осуществляют обучение и инструктаж работников Учреждения, внутренний контроль за соблюдением Учреждением и его работниками требований к защите ПДн;

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

6.5.3. Разработка Политики в отношении обработки и защиты персональных данных и иных организационно-распорядительных документов в области обработки и защиты персональных данных;

6.5.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

6.5.5. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности;

6.5.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

6.5.7. Сертифицированное программное средство защиты информации от несанкционированного доступа;

6.5.8. Сертифицированные межсетевой экран и средство обнаружения вторжения;

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

6.5.10. Установление правил доступа к обрабатываемым ПДн, к помещениям, предназначенным для обработки ПДн; обеспечение регистрации и учета действий, совершаемых с ПДн в ИСПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

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

6.5.12. Ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации в сфере

обработки и защиты персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими Политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;

6.5.13. Осуществление внутреннего контроля и аудита.

7. Основные права субъекта ПДн и обязанности Учреждения

7.1. Основные права субъекта ПДн

7.1.1. Субъект ПДн за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 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 Федеральным законом «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 июля 2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

7.1.2. 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.

7.2. Обязанности Учреждения

Учреждение обязано:

- при сборе ПДн предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Если ПДн были получены не от субъекта ПДн, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», предоставить субъекту ПДн следующую информацию:
    1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
    2) цель обработки персональных данных и ее правовое основание;
    3) предполагаемые пользователи персональных данных;
    4) установленные настоящим Федеральным законом права субъекта персональных данных;
    5) источник получения персональных данных.
- разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн, если предоставление ПДн является обязательным в соответствии с федеральным законом;
- 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.

Согласовано,
нач. юр. отд.
А.В. Яковлев