Приложение 1 к приказу
Главного врача ГБУЗ ЛО
«Тосненская КМБ» № 263 от
28 июля 2023г.

ПОЛИТИКА
ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
в Государственном бюджетном учреждении здравоохранения Ленинградской области «Тосненская клиническая межрайонная больница»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с пунктом 2 статьи 18.1 Закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных» и является основополагающим внутренним регулятивным документом медицинского Учреждении Государственное бюджетное учреждение здравоохранения Ленинградской области «Тосненская клиническая межрайонная больница» (далее – Учреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПДн), оператором которых является Учреждение.

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 Учреждении, в том числе защиты прав на неприкосновенность частной, личной, семейной жизни и врачебной 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 ее утверждения.

1.4. Обработка ПДн в Учреждении осуществляется в связи с оказанием Организацией медицинских услуг, определяемых:

– Законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя (гл. 14 ТК РФ), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. 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 утверждения приказом руководителя учреждения, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Учреждения по адресу: 187000, г. Тосно, шоссе Барыбина, дом 29, а электронная версия Политики – на сайте по адресу www.tosnocrb.ru.

2. 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.

Субъект ПДн - это любое физическое лицо, обладающее соответствующими 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 (ИСПД) – 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.
Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.
Медицинский работник – специалист, на которого возложены, учреждением функции по непосредственному участию в оказании пациенту медицинской помощи в период наблюдения за ним и его лечения.

3.Принципы обеспечения безопасности персональных данных

3.1. 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.
3.2. 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 информационныхтехнологий, 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 информационных систем персональных данных Учреждении, 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 Учреждении 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 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 Организацией ПНд уничтожатся или обезличиваются.

3.4. При обработке ПДн обеспечиваются их достоверность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уточнению неполных, или неточных ПДн. 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 уведомлен об этом и от него должно быть получено согласие.

4.1.2. Учреждение должно 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 путем:
а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН,пенсионное свидетельство и т. д.);
б) внесения сведений в учетные формы;
в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение,характеристика и т. д.).
Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Учреждением, определяется в соответствии сзаконодательством и определяется внутренними регулятивными документами Учреждении.

4.2. Обработка ПДн

4.2.1. Обработка персональных данных осуществляется:

- с согласия субъекта персональных данных на обработку его персональных данных, с каждым работником Учреждения подписывается согласие на обработку персональных данных по типовой форме в соответствии с Приложением 2 к настоящей Политике.

- с каждым субъектом ПДн, нуждающимся в медицинской помощи или получающим (получившим) медицинскую помощь в Учреждении подписывается Согласие на обработку персональных данных по типовой форме, утвержденной приказом Главного врача.

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения предусмотренных 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 подпись знакомятся с документами Учреждения, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

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

4.2.2. Цели обработки ПДн:

– Обеспечение Учреждением оказания медицинской помощи населению, а также наиболее полного исполнения обязательств в соответствии с законами от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 г. N61-ФЗ «Об обращении лекарственных средств», N 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими Учреждениями платных медицинских услуг, утвержденными постановлением Правительства РФ, от 4 октября 2012 г. N 1006 «Об утверждении правил предоставления медицинскими организациями платных медицинских услуг» ;

– Осуществление трудовых отношений;

– Осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных

В Учреждении обрабатываются ПДн следующих субъектов:

– физические лица, состоящие с учреждением в трудовых отношениях;

– физические лица, являющие близкими родственниками сотрудников учреждения;

– физические лица, уволившиеся из учреждения;

– физические лица, являющиеся кандидатами на работу;

– физические лица, состоящие с учреждением в гражданско-правовых отношениях;

– физические лица, обратившиеся в учреждение за медицинской помощью.

4.2.4. ПДн, обрабатываемые Учреждением:

– полученные при осуществлении трудовых отношений;

– полученные для осуществления отбора кандидатов на работу в учреждение;

– полученные при осуществлении гражданско-правовых отношений;

– полученные при оказании медицинской помощи.

4.2.5. Обработка персональных данных ведется:

– с использованием средств автоматизации;

– без использования средств автоматизации.

4.2.6. К Политике прилагается утвержденный перечень ПДн, обрабатываемых в ГБУЗ ЛО "Тосненская КМБ" (приложение 1).

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

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

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

4.3.4. Хранение ПДн в форме, позволяющей определить личность субъекта ПДн, осуществляется не дольше, чем этоготребуют 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 путем 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 путем 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. Учреждение передает ПДн третьим лицам в следующих случаях:

– субъект выразил свое согласие на такие действия;

– передача предусмотрена законодательством РФ.

4.5.2. Перечень третьих лиц, которым передаются ПДн:

– Социальный фонд России (на законных основаниях);

– Налоговые органы РФ (на законных основаниях);

– Территориальный фонд обязательного медицинского страхования (на законных основаниях);

– страховые медицинские Учреждении 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;

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Учреждением 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. В целях обеспечения сохранности и конфиденциальности персональных данных Субъектов персональных данных Учреждения все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только определенными работниками Учреждении, осуществляющими работу в соответствии со своими должностными обязанностями, и подписавшими **«Обязательство о неразглашении персональных данных»**, в соответствии с Приложением 3 к настоящей Политике.

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

5.5. Основными мерами защиты ПДн, используемыми Учреждением, 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. Проведение контроля обеспечения безопасности и обработки персональных данных, не реже одного раза в год.

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

5.5.4. Разработка политики в отношении обработки персональных данных.

5.5.5. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПД.

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

5.5.7. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности.
5.5.8. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
5.5.9. Сертифицированное программное средство защиты информации от несанкционированного доступа.
5.5.10.Сертифицированные межсетевой экран и средство обнаружения вторжения. Соблюдение условий, обеспечивающих сохранность ПДн и исключающих 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 учета 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 Учреждении, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Учреждении в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.
5.5.14.Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПДн и обязанности Учреждения

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 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 настоящим 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.

6.2. Обязанности Учреждения

Учреждение обязано:
– при сборе ПДн предоставить информацию субъекту об обработке его ПДн;

– в случаях, если ПДн были получены не от субъекта ПДн, уведомить субъекта;
– 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 позащите прав субъектов ПДн.

7. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.

7.1 Документы, содержащие персональные данные, сроки хранения которых истекли, подлежат уничтожению в порядке, предусмотренном нормативными правовыми актами Российской Федерации В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональных данных или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

7.2 Лицами, ответственными за архивную обработку документов в Учреждении, осуществляется систематический контроль за выделением документов на бумажных носителях, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

7.3 Сведения об уничтожении вносятся в Акт об уничтожении документов.

7.4 Уничтожение персональных данных на электронных носителях производится под контролем работников подразделений информационных технологий Учреждения 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.

7.5 Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

7.6 Уничтожение персональных данных, не подлежащих архивному хранению, осуществляется только комиссией в составе представителя структурного подразделения (или работника), ответственного за защиту персональных данных и представителя структурного подразделения, в чьем ведении находятся указанные персональных данные. По результатам уничтожения оформляется Акт.

8. Ответственность за разглашение информации, связанной с персональными данными

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

8.2 Работник, которому в силу трудовых отношений с Учреждением стала известна информация, составляющая персональные данные, в случае нарушения режима защиты этих персональных данных несет дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами Российской Федерации.

8.3 Разглашение персональных данных субъектов персональных данных (передача их

посторонним лицам, в том числе работникам Учреждения, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящей Политикой, локальными нормативными актами (приказами, распоряжениями) Учреждения, может повлечь наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания, если иное не предусмотрено законодательством РФ.