

**ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ
«ВЯЗЕМСКАЯ ГОРОДСКАЯ СТОМАТОЛОГИЧЕСКАЯ ПОЛИКЛИНИКА»**

УТВЕРЖДАЮ
Главный врач
_____ Л.С.Педан
« 16 » июня 2017г

**Политика обработки и защиты персональных данных медицинской
организации ОГАУЗ «Вяземская городская стоматологическая
поликлиника»**

1. Общие положения

1.1. Настоящая политика в отношении обработки персональных данных составлена в соответствии с п.2 ст18.1 Федерального закона №152-ФЗ от 27.07.2006г «О персональных данных» и является основополагающим внутренним регулятивным документом ОГАУЗ «Вяземская городская стоматологическая поликлиника», определяющим ключевые направления его деятельности в области обработки и защиты персональных данных, оператором которых является Учреждение.

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

1.3. Положения Политики распространяются на отношения по обработке и защите персональных данных, 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 персональных данных, полученных до ее утверждения.

1.4. Обработка персональных данных в учреждении осуществляется в связи с выполнением Учреждением функций, предусмотренных ее учредительными документами, и определяемых:

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

- Постановление Правительства РФ от 01.11.2012г. № 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 персональных данных в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя (гл.14 Трудового кодекса РФ), в связи с реализацией Учреждением 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 ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Учреждения по адресу: Смоленская область, Вяземский район, г. Вязьма, ул. Парижской Коммуны, д.8, электронная версия Политики - на сайте по адресу: stomvuzazma.zdrav.admin-smolensk.ru.

2. Термины и принятые сокращения

Персональные данные - 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, 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 - совокупность содержащихся в базе 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.

Лечащий врач - врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3. Принципы обеспечения безопасности персональных данных.

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

3.2. Для обеспечения безопасности персональных данных Учреждение руководствуется следующими принципами:

- *законность*: защита персональных данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты персональных данных;

- *системность*: обработка персональных данных в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и фактов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных;

- *комплексность*: защита персональных данных строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения и других имеющихся в Учреждении систем и средств защиты;
- *непрерывность*: защита персональных данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки персональных данных, в том числе при проведении ремонтных и регламентированных работ;
- *своевременность*: меры, обеспечивающие надлежащий уровень безопасности персональных данных, принимаются до начала их обработки;
- *преемственность и непрерывность совершенствования*: модернизация и наращивание мер и средств защиты персональных данных осуществляется на основании результатов анализа практики обработки персональных данных в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности персональных данных, отечественного и зарубежного опыта в сфере защиты информации;
- *персональная ответственность*: ответственность за обеспечение безопасности персональных данных возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой персональных данных;
- *минимизация прав доступа*: доступ к персональным данным предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- *гибкость*: обеспечение выполнения функций защиты персональных данных при изменении характеристик функционирования информационных систем персональных данных Учреждения, а также объема и состава обрабатываемых персональных данных;
- *специализация и профессионализм*: реализация мер по обеспечению безопасности персональных данных осуществляется Работниками, имеющими необходимые 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 персональных данных;
- *наблюдаемость и прозрачность*: меры по обеспечению безопасности персональных данных 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 персональных данных, а результаты контроля регулярно анализируются.

3.3. В Учреждении не производится обработка персональных данных, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки персональных данных в Учреждении, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшихся Учреждением персональные данные уничтожаются или обезличиваются.

3.4. При обработке персональных данных обеспечивается их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уничтожению неполных или неточных персональных данных.

4. Обработка персональных данных

4.1. Получение персональных данных

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

4.1.2. Учреждение (оператор) должно сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных, перечне действий с персональными данными, 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 персональные данные, создаются путем:

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

Порядок доступа субъекта персональных данных к его персональным данным, обрабатываемым Учреждением, определяется в соответствии с законодательством и внутренними регулятивными документами Учреждения.

4.2. Обработка персональных данных

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 законодательством РФ 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 персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

Допущенные к обработке персональных данных Работники под роспись знакомятся с документами учреждения, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных работников.

Учреждением производится устранение выявленных нарушений законодательства об обработке и защите персональных данных.

4.2.2. Цели обработки персональных данных:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21.11.2011г № 323-ФЗ №Об основах охраны здоровья граждан РФ», от 12.04.2010г № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010г № 326-ФЗ «Об обязательном медицинском страховании граждан в российской федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства РФ от 04.10.2012г. №1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных.

В Учреждении обрабатываются персональные данные следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся их 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. Персональные данные, обрабатываемые Учреждением:

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу в Учреждение;
- данные, полученные при осуществлении гражданско-правовых отношений;
- данные, полученные при оказании медицинской помощи.

Полный список персональных данных представлен в Перечне персональных данных, утвержденном главным врачом Учреждения.

4.2.5. Обработка персональных данных ведется:

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

4.3. Хранение персональных данных

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

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

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

4.3.4. Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) в информационной системе персональных данных.

4.3.5. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, 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 персональных данных.

4.4.1. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

4.4.2. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

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

4.5. Передача персональных данных

4.5.1. Учреждение передает персональные данные третьим лицам в следующих случаях:

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

4.5.2. Перечень лиц, которым передаются персональные данные

Третьи лица, которым передаются персональные данные:

- Пенсионный фонд РФ для учета (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;
- банки для начисления заработной платы (на основании договора);
- 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).

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Учреждением создана система защиты персональных данных, 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 системы защиты персональных данных.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления системы защиты персональных данных, разрешительной системы, защиты информации при работе с сотрудниками, партнерами 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 персональных данных.

5.5. Основными мерами защиты персональных данных, используемыми Учреждением, являются:

5.5.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите персональных данных.

5.5.2. Определение актуальных угроз безопасности персональных данных при их обработке в информационной системе персональных данных, и разработка мер и мероприятий по защите персональных данных.

5.5.3. Разработка политики в отношении обработки персональных данных.

5.5.4. Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

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

5.5.6. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации, учет машинных носителей персональных данных, 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 персональных данных и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности персональных данных.

5.5.11. Установление правил доступа к обрабатываемым персональным данным, обеспечение регистрации и учета действий, совершаемых с персональными данными, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

5.5.12. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.5.13. Обучение работников Учреждения, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Учреждения в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

5.5.14. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта персональных данных и обязанности Учреждения

6.1. Основные права субъекта персональных данных

Субъект 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 настоящим Федеральным законом или другими федеральными законами.

Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случаях, 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 персональных данных предоставить информацию об обработке его персональных данных;
- в случаях если персональные данные были получены не от субъекта персональных данных уведомить субъекта;

- при отказе в предоставлении персональных данных субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- давать ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.