5.1. Настоящая Политика в отношении обработки персональных данных(далее — Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональныхданных» и является основополагающим внутренним регулятивным документом медицинской организации ООО БИОС (далее Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее — ПДн), оператором которых является Организация.

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

5.3. Положения Политики распространяются на отношения по обработкеи защите ПДн, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики немогут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

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

4 Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основахохраны здоровья граждан в Российской Федерации»;

5 Постановлением Правительства РФ от 04.10.2012 №1006 «Об утверждении Правил предоставления медицинскими организациямиплатных медицинских услуг»;

6 Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

7 Постановлением Правительства Российской Федерации от 15 сентября2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использованиясредств автоматизации»;

8 Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Обутверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

9 иными нормативными правовыми актами Российской Федерации.Кроме того, обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14Трудового кодекса Российской Федерации), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

5.5. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается

дата последнего обновления редакции. Новая редакция Политикивступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.
5.6. Действующая редакция хранится в месте нахождения Организации по адресу:620034, Свердловская область, г. Екатеринбург, ул. Готвальда6\1 пом.№42. Электронная версия Политики — на сайте по адресу: prior-m.ru.

6 Термины и принятые сокращения

Персональные данные (ПДн) — любая информация, относящаяся кпрямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
Обработка персональных данных — любое действие (операция) илисовокупность 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 сдругими 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, направленныена 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 прекращениеобработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
Уничтожение персональных данных — действия, в результатекоторых становится невозможным восстановить содержание
персональных данных в информационной системе персональных данныхи (или) в результате которых уничтожаются материальные носители персональных данных;
Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительнойинформации определить принадлежность персональных данных конкретному субъекту персональных данных;
Автоматизированная обработка персональных данных —
обработка персональных данных с помощью средств вычислительнойтехники;
Информационная система персональных данных (ИСПД) — совокупность содержащихся в базах данных персональных данных и

обеспечивающих их обработку информационных технологий итехнических 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 медицинскойпомощи в период наблюдения за ним и его лечения.

7 Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступак 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 руководствуетсяследующими принципами:
10 законность: защита ПДн основывается на положениях нормативныхправовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;
11 системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времениэлементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
12 комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и другихимеющихся в Организации систем и средств защиты;
13 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;
14 своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
15 преемственность и непрерывность совершенствования: модернизацияи наращивание мер и средств защиты ПДн осуществляется на основаниирезультатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
16 персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
17 минимизация прав доступа: доступ к ПДн предоставляется Работникам

только в объеме, необходимом для выполнения их должностных обязанностей;
18 гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных системперсональных данных Организации, а также объема и состава
обрабатываемых ПДн;
19 специализация и профессионализм: реализация мер по обеспечениюбезопасности ПДн осуществляются Работниками, имеющими
необходимые для этого квалификацию и опыт;
20 эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и
мотивацию Работников, позволяющую исключить или минимизироватьвозможность нарушения ими безопасности ПДн;
21 наблюдаемость и прозрачность: меры по обеспечению безопасностиПДн должны быть спланированы так, чтобы результаты их применениябыли явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
22 непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, арезультаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, поокончании обработки ПДн в Организации, 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 точность, достаточность, а при необходимости — и актуальность по отношению к целям обработки.Организация принимает необходимые меры по удалению или уточнениюнеполных или неточных ПДн.

8 Обработка персональных данных

- Получение ПДн
- Все ПДн следует получать от самого субъекта. Если ПДн субъектаможно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.
- Оператор должен сообщить субъекту о целях, предполагаемыхисточниках 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 отказасубъекта дать письменное согласие на их получение.
- Документы, содержащие ПДн создаются путем:

а) копирования 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 Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

- Обработка ПДн
- Обработка персональных данных осуществляется:

23 с согласия субъекта персональных данных на обработку его персональных данных;
24 в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
25 в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектомперсональных 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 Организации.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретныхРаботников.
Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

- Цели обработки ПДн:

26 обеспечение организации 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 29ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинскихуслуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;
27 осуществление трудовых отношений;
28 осуществление гражданско-правовых отношений;
29 для связи с пользователями сайта, в том числе путем направления уведомлений, запросов и информации, касающихся использования сайта, оказания медицинской помощи, анализа РИ в стоматологии;
30 обезличивания персональных данных для получения обезличенных статистических данных, которые передаются третьему лицу для проведения исследований, выполнения работ или оказания услуг по поручению Клиники.

- Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов:
31 физические лица, состоящие с Организацией в трудовых отношениях;
32 физические лица, являющие близкими родственниками сотрудниковОрганизации;
33 физические лица, уволившиеся из Организации;
34 физические лица, являющиеся кандидатами на работу;
35 физические лица, состоящие с Организацией в гражданско-правовыхотношениях;

36 физические лица, обратившиеся в Организацию за медицинскойпомощью;
37 физические лица, являющиеся пользователями сайта prior-m.ru.

- ПДн, обрабатываемые Организацией:

38 данные полученные при осуществлении трудовых отношений;
39 данные полученные для осуществления отбора кандидатов на работув организацию;
40 данные полученные при осуществлении гражданско-правовыхотношений;
41 данные полученные при оказании медицинской помощи;
42 данные, полученные от пользователя сайта prior-m.ru.

Полный список ПДн представлен в Перечне ПДн, утвержденномдиректором Организации.

- Обработка персональных данных ведется:

43 с использованием средств автоматизации;
44 без использования средств автоматизации.

- Хранение ПДн
- ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, таки в электронном виде.
- ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченнымправом доступа.
- ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).
- Не допускается хранение и размещение документов, содержащихПД, в открытых электронных каталогах (файлообменниках) в ИСПД.
- Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и ониподлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.
- Уничтожение ПДн
- Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химическогоразложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.
- ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.
- Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.
- Передача ПДн
- Организация передает ПДн третьим лицам в следующих случаях:

45 субъект выразил свое согласие на такие действия;
46 передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательствомпроцедуры.

- Перечень лиц, которым передаются ПДн Третьи лица, которым передаются ПДн:

47 Пенсионный фонд РФ для учета (на законных основаниях);
48 Налоговые органы РФ (на законных основаниях);
49 Фонд социального страхования (на законных основаниях);
50 Территориальный фонд обязательного медицинского страхования (назаконных основаниях);
51 страховые медицинские организации по обязательному и
добровольному медицинскому страхованию (на законных основаниях);
52 банки для начисления заработной платы (на основании договора);
53 судебные и правоохранительные органы в случаях, установленных законодательством;
54 бюро кредитных историй (с согласия субъекта);
55 юридические фирмы, работающие в рамках законодательства РФ, принеисполнении обязательств по договору займа (с согласия субъекта).

9 Защита персональных данных

1.1. В соответствии с требованиями нормативных документов
Организацией создана система защиты персональных данных (СЗПД),состоящая из подсистем правовой, организационной и технической защиты.
1.2. Подсистема правовой защиты представляет собой комплексправовых, организационно-распорядительных и нормативных
документов, обеспечивающих создание, функционирование и
совершенствование СЗПД.
1.3. Подсистема организационной защиты включает в себя организациюструктуры управления СЗПД, разрешительной системы, защиты
информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.
1.4. Подсистема технической защиты включает в себя комплекс
технических, программных, программно-аппаратных средств,
обеспечивающих защиту ПДн.
1.5. Основными мерами защиты ПДн, используемыми Организацией,являются:

- Назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением Организацией и его работникамитребований к защите ПДн;
- Определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;
- Разработка политики в отношении обработки персональныхданных;
- Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых сПДн в ИСПД;
- Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
- Применение средств защиты информации, учет машинныхносителей ПДн, обеспечение их сохранности;

- Антивирусное программное обеспечение с регулярно обновляемыми базами;
- Программное средство защиты информации от несанкционированного доступа;
- Межсетевой экран и средство обнаружения вторжения;
- Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечениюбезопасности ПДн;
- Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а такжеобнаружение фактов несанкционированного доступа к персональным данным и принятия мер;
- Восстановление ПДн, модифицированных или уничтоженныхвследствие несанкционированного доступа к ним;
- Обучение работников Организации непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в томчисле требованиям к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;
- Осуществление внутреннего контроля и аудита.

10 Основные права субъекта ПДн и обязанности Организации

- Основные права субъекта ПДн

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

56 подтверждение факта обработки персональных данных оператором;

57 правовые основания и цели обработки персональных данных;

58 цели и применяемые оператором способы обработки персональныхданных;

59 наименование и место нахождения оператора, сведения о лицах (заисключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональныеданные на основании договора с оператором или на основании федерального закона;

60 обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник ихполучения, если иной порядок представления таких данных не предусмотрен федеральным законом;

61 сроки обработки персональных данных, в том числе сроки иххранения;

62 порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

63 информацию об осуществленной или о предполагаемой трансграничной передаче данных;

64 наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению

оператора, если обработка поручена или будет поручена такому лицу;
65 иные сведения, предусмотренные настоящим Федеральным закономили другими федеральными законами.
Субъект ПДн вправе требовать от оператора уточнения его
персональных данных, их блокирования или уничтожения в случае, еслиперсональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленнойцели обработки, а также принимать предусмотренные законом меры по защите своих прав.

- Обязанности Организации

Организация обязана:
66 при сборе ПДн предоставить информацию об обработке его ПДн;
67 в случаях если ПДн были получены не от субъекта ПДн уведомитьсубъекта;
68 при отказе в предоставлении ПДн субъекту разъясняются последствиятакого отказа;
69 опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, ксведениям о реализуемых требованиях к защите ПДн;
70 принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерногоили случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн;
71 давать ответы на запросы и обращения субъектов ПДн, их
представителей и уполномоченного органа по защите прав субъектовПДн.