Приложение 3
к приказу от 04.11.2018 г. № 79

**УТВЕРЖДАЮ**
Главный врач БУЗ ВО «Вологодский областной кожно-венерологический диспансер № 2»

_____ Е.Г. Максимова
«___» _____ 2018 г.

**Политика обработки и защиты персональных данных БУЗ ВО «Вологодский областной кожно-венерологический диспансер №2»**

**1.Общие положения**

1.1. Настоящая Политика в отношении обработки персональных данных(далее Политика) составлена в соответствии с п2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006г «О персональных данных» и является основополагающим внутренним регулятивным документом БУЗ ВО «Вологодский областной кожно-венерологический диспансер №2»(далее Организация), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных(далее по тексту – ПДн),оператором которых является Организация.

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

1.3. Политика распространяется на отношения по обработке и защите персональных данных, полученных Организацией как до, так и после утверждения настоящей Политики.

1.4.Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.5. Организация публикует Политику в свободном доступе, размещая ее на своем официальном сайте в информационно-телекоммуникационной сети "Интернет", на бумажном носителе действующая редакция хранится по юридическому адресу Вологодская область, г. Череповец, ул. Чкалова 16.

**2. Правовые основания обработки персональных данных**

2.1 Обработка ПДн в Организации осуществляется в связи с выполнением функций, предусмотренных ее учредительными документами и определяемых%

-Конституцией Российской Федерации;

- Статьями 86-90 Трудового кодекса Российской Федерации;

- Статьей 6 (пункт 2 части 1) Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных";

-Федеральным законом от 21.11.2011г №323 «Об основах охраны здоровья граждан в российской Федерации»;

-Постановлением правительства Российской Федерации от 15.09.2008г №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

-Постановлением правительства Российской Федерации от 01.11.2012г №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

-Иными нормативными правовыми актами РФ.

2.2 Обработка ПДн в организации осуществляется в ходе трудовых и иных непосредственно связанных с ним отношений, в которых организация выступает в качестве работодателя, в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

**3.Принципы обеспечения безопасности персональных данных**

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

3.2.Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

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

-системность: обработка ПДн в Организации осуществляется с 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 Организации и других имеющихся в Организации систем и средств защиты;

-непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

-своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
-преемственность и совершенствование: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практик обработки ПДн в Организации 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 Работника 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 Организации, а так же объёма и состава обрабатываемых ПДн;
-специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляется Работниками, имеющими необходимые для этого квалификацию и опыт;
-эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
-наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы и могли быть оценены лицами, осуществляющими контроль;
-непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.
3.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.
3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости — и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

## 4. Обработка персональных данных

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

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.
4.1.3. Документы, содержащие ПДн создаются путем:
- копирования оригиналов документов(паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
-внесения сведений в учетные формы;
- получения оригиналов необходимых документов(трудовая книжка, медицинское заключение, характеристика и др.);
Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

**4.2. Обработка Персональных данных**
4.2.1. Обработка ПДн осуществляется:
- с согласия субъекта ПДн на обработку его персональных данных;
- в случаях, когда обработка ПДн необходима для осуществления и выполнения возложенных законодательством РФ функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе(далее- персональные данные, сделанные общедоступными субъектом ПДн).

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, устанавливающими права и обязанности конкретных Работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.
4.2.2. Цели обработки ПДн:
- обеспечение организации оказания медицинской помощи наслоению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 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 РФ», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерацией от 04.10.2012г № 1006;
- осуществление трудовых отношений;

-осуществление гражданско-правовых отношений.
4.2.3. Категории субъектов персональных данных:
- физические лица, состоящие с Организацией в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников Организации;
- физические лица, уволившиеся из Организации;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с Организацией в гражданско-правовых отношениях;
- физические лица, обратившиеся в организацию за медицинской помощью.
4.2.4.Пдн, обрабатываемые Организацией:
- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу в Организацию;
- данные, полученные при осуществлении гражданско-правовых отношений;
- данные, полученные при оказании медицинской помощи.
Полный список ПДн представлен в Перечне ПДн, утвержденным главным врачом Организации.
4.2.5. Обработка персональных данных ведется:
- с использованием средств автоматизации;
- без использования средств автоматизации.

**4.3. Хранение Персональных данных**

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде;
4.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа(кабинет отдела кадров, регистратура, архив);
4.3.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в электронном виде на защищенном локальном сервере;
4.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПД;
4.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

**4.4. Уничтожение ПДн**

4.4.1. Уничтожение документов(носителей),содержащих ПДн производится в установленные законом сроки 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 проводится комиссией. Факт уничтожения ПДн подтверждаются документально актом об уничтожении носителей, подписанным членами комиссии.

**4.5. Передача ПДн**

4.5.1. Организация передает ПДн 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 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);
-Судебные и правоохранительные органы в случаях, установленных законодательством.

**5.Защита персональных данных**

5.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных(СЗПД), состоящая из подсистем правовой , организационной и технической защиты;
5.2. Подсистема правовой защиты представляет собой комплекс правовых , организационно-распорядительных и нормативных документов, обеспечивающих создание. Функционирование и совершенствование СЗПД;
5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы ,защиты информации при работе с 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 ПДн;
5.5. Основными мерами защиты ПДн, используемыми Организацией, являются:
5.5.1. Назначение лица, ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;

5.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД и разработка мер , и мероприятий по защите ПДн;
5.5.3. Разработка политики в отношении обработки ПДн;
5.5.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий. Совершаемых с ПДн в ИСПД;
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 процедуру оценки соответствия средств защиты информация, учет машинных носителей ПДн, обеспечение их сохранности;
5..5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
5.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;
5.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;
5.5.10. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;
5.5.11. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий , совершаемых с Пдн, а также обнаружение фактов несанкционированного доступа к ПДн и принятия мер;
5.5.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ПДн и принятия мер;
5.5.13. Обучение Работников Организации непосредственно осуществляющих обработку ПДн, положениям законодательства РФ о персональных данных, в том числе требованиям к защите ПДн, документами, определяющим политику Организации в отношении обработки ПДн, локальным актам по вопросам обработки ПДн;
5.5.14. Осуществление внутреннего контроля и аудита.

**6.Основные права субъекта ПДн и обязанности Организации**

6.1. Субъект ПДн имеет право на получение информации, касающиеся обработки его ПДн, в том числе содержащей:
- подтверждение факта обработки ПДн оператором;
-правовые основания и цели обработки ПДн;
-цели и применяемые оператором способы обработки ПДн;
-наименование и место нахождения оператора, сведения о лицах ( за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;

- обрабатываемые ПДн , относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных ФЗ « О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн вправе требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн 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 Организации:
- при сборе ПДн предоставить информацию 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, представления, 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.

6.3. Ответственность работников Организации, осуществляющих обработку персональных данных и имеющих право доступа к ним, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Организации.