УТВЕРЖДАЮ

Главный врач БУЗ ВО «ВОИБ»

_____ Л.В. Розин

«___» _____ 2017 года

Политика обработки и защиты персональных данных

бюджетного учреждения здравоохранения Вологодской области

«Вологодская областная инфекционная больница»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и является основополагающим внутренним регулятивным документом бюджетного учреждения здравоохранения Вологодской области «Вологодская областная инфекционная больница» (далее - БУЗ ВО «ВОИБ», Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПД), 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 БУЗ ВО «ВОИБ», в том числе защиты прав на неприкосновенность частной жизни, личной, семейной, врачебной тайны.

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 ходе трудовых и иных, непосредственно связанных с ними отношений, где БУЗ ВО «ВОИБ» выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), и 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 утверждения.

1.6. Действующая редакция хранится в отделе кадров по месту нахождения БУЗ ВО «ВОИБ» по адресу: Вологодская область, г. Вологда, ул. Пошехонское шоссе, д. 30, электронная версия Политики – на сайте по адресу: voib.volmed.org.ru

2. Правовые основания обработки персональных данных

Политика БУЗ ВО «ВОИБ» в области обработки и защиты персональных данных определяется следующими основными нормативными правовыми актами Российской Федерации:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
- Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»;
- Федеральный закон от 01.04.1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральный закон от 24.07.2009 г. № 212-ФЗ «О страховых взносах в Пенсионный Фонд Российской Федерации, Фонд социального страхования

Российской Федерации, Федеральный Фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;

- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- Федеральный закон от 22.10.2004г. № 125-ФЗ «Об архивном деле в Российской Федерации»;

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

- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»;

- Иными нормативными правовыми актами.

3. Термины и принятые сокращения

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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;

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;

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;

Трансграничная передача ПД – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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.

4. Принципы обеспечения безопасности персональных данных

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

4.2. Для обеспечения безопасности ПД Оператор руководствуется следующими принципами:

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

– системность: обработка ПД в учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД;

– комплексность: защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Оператора, и других имеющихся в учреждении систем и средств защиты;

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

– своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;

– преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляется на основании результатов анализа практики обработки ПД в учреждении с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;

– персональная ответственность: ответственность за обеспечение безопасности и конфиденциальности ПД возлагается на Работников учреждения в пределах их обязанностей, связанных с обработкой и защитой ПД;

– минимизация прав доступа: доступ к ПД предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

– гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных учреждения, а также объема и состава обрабатываемых ПД;

– специализация и профессионализм: реализация мер по обеспечению безопасности ПД осуществляется 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 ПД;

– наблюдаемость и прозрачность: меры по обеспечению безопасности ПД 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 ПД, а результаты контроля регулярно анализируются.

4.3. Оператор не производит обработку ПД, несовместимую с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД в учреждении, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся учреждением ПД уничтожаются или обезличиваются.

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

5.Обработка персональных данных

5.1. Получение Персональных Данных

5.1.1. Все ПД следует получать от самого субъекта. Если ПД 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 ПД, характере подлежащих получению ПД, перечне действий с ПД и 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 ПД создаются путем:

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

б) внесения сведений в учетные формы;

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

Порядок доступа субъекта персональных данных к его ПД, обрабатываемым оператором, определяется в соответствии с законодательством и определяется внутренними регулятивными документами учреждения.

5.2. Обработка ПД

5.2.1. Обработка персональных данных осуществляется:

– на законной и справедливой основе;

– с согласия субъекта ПД на обработку его персональных данных;

– в случаях, когда обработка персональных данных необходима для осуществления и исполнения, 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 ПД).

Доступ Работников к обрабатываемым ПД 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 ПД, включая документы, устанавливающие права и обязанности конкретных работников.

Учреждение производит устранение выявленных нарушений законодательства в сфере обработки и защиты персональных данных.

5.2.2 Цели обработки ПД:

– обеспечение организацией оказания доступной и качественной медицинской помощи населению, а также наиболее полного исполнения

обязательств и компетенций в соответствии с Федеральными законами от 21.11. 2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 04.10.2012 № 1006;

– осуществление трудовых отношений;

– осуществление гражданско-правовых отношений.

5.2.3. Категории субъектов персональных данных

В учреждении обрабатываются ПД 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.

5.2.4. Персональные данные, обрабатываемые в учреждении:

– 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 персональных данных представлен в Перечне персональных данных.

5.2.5. Обработка персональных данных ведется:

– с использованием средств автоматизации.

– без использования средств автоматизации.

5.3. Хранение ПД

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

5.3.2. ПД, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

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

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

5.3.5. Хранение ПД в форме, позволяющей определить субъекта ПД, 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.

5.4. Уничтожение ПД

5.4.1. Уничтожение документов (носителей), содержащих ПД производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

5.4.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

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

5.5. Передача ПД

4.5.1. Учреждение передает ПД третьим лицам в следующих случаях:

– субъект выразил свое согласие на такие действия;

– передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

5.5.2. Перечень лиц, которым передаются ПД

Третьи лица, которым передаются ПД:

– 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;

– бюро кредитных историй (с согласия субъекта);

– юридические фирмы, адвокаты, работающие в рамках законодательства РФ (с согласия субъекта), в том числе, при неисполнении обязательств по договору займа.

6. Защита персональных данных

6.1. В соответствии с требованиями нормативных документов учреждением 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 организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами, контрагентами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

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

6.5. Основными мерами защиты ПД, используемыми оператором, являются:

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

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

6.5.3. Разработка политики в отношении обработки персональных данных;

6.5.4. Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в ИСПД;

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

6.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПД, обеспечение их сохранности;

6.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

6.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа;

6.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения;

6.5.10. Соблюдение условий, обеспечивающих сохранность ПД и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПД;

6.5.11. Установление правил доступа к обрабатываемым ПД, обеспечение регистрации и учета действий, совершаемых с ПД, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

6.5.12. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

6.5.13. Обучение работников учреждения, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику учреждения в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

6.5.14. Осуществление внутреннего контроля и аудита.

7. Основные права субъекта ПД и обязанности Оператора

7.1. Основные права субъекта ПД

Субъект ПД 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 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

Субъект ПД 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 Оператора

учреждение обязано:

– при сборе ПД предоставить информацию об обработке ПД;

– в случаях если ПД были получены не от субъекта ПД уведомить субъект;

– при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;

– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;

– принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД а также от иных неправомерных действий в отношении ПД;

– давать ответы на запросы и обращения субъектов ПД, их законных представителей и уполномоченного органа по защите прав субъектов ПД.

8. Заключительные положения

8.1 Настоящая Политика является внутренним документом Оператора, общедоступной и подлежит обнародованию на официальном сайте учреждения.

8.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не чаще одного раза в три года.

8.3. Внутренний контроль за соблюдением локальных нормативных актов БУЗ ВО «ВОИБ» в области персональных данных, в том числе, требований к защите персональных данных, осуществляется лицом (-ами), определенными приказом главного врача.

8.4. Ответственность должностных лиц Оператора, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации.