

ПОЛИТИКА
в отношении обработки персональных данных
в бюджетном учреждении здравоохранения Вологодской области
«Вологодская областная психиатрическая больница»

1. Общие положения

1.1. Настоящая политика в отношении обработки персональных данных (далее – Политика) разработана Бюджетным учреждением здравоохранения Вологодской области «Вологодская областная психиатрическая больница» (далее – Оператор) в целях исполнения требований Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных».

1.2. Политика определяет общий порядок, принципы и условия обработки персональных данных Оператором и защищает права субъектов персональных данных на неприкосновенность частной жизни, личную и семейную тайну в процессе обработки их персональных данных.

1.3. Целью настоящей Политики является обеспечение безопасности объектов защиты Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

1.4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.5. Требования настоящей Политики распространяются на всех сотрудников Учреждения (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

1.6. Основные понятия, используемые в Политике

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Субъект персональных данных - физическое лицо, данные которого обрабатываются;

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Оператор персональных данных (Оператор) – медицинское учреждение, самостоятельно или совместно с другими лицами организующее и (или)

осуществляющее обработку персональных данных, а также определяющее цели обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка включает сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

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;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

1.7. Основные права и обязанности Оператора персональных данных

1.7.1. Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных.

1.7.2. Если предоставление персональных данных субъектом Оператору является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

1.7.3. При сборе персональных данных, Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных Федеральном законе «О персональных данных».

1.7.4. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных, а в случае осуществления сбора персональных данных с использованием сети Интернет обязан опубликовать в соответствующей информационно-телекоммуникационной сети Политику и сведения о реализуемых требованиях к защите персональных данных.

1.7.5. Оператор при обработке персональных данных обязан 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, а также от иных неправомерных действий в отношении персональных данных.

1.7.6. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

1.8. Основные права и обязанности субъекта персональных данных

1.8.1. Субъект персональных данных 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.

1.8.2. Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, разрешается только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

1.8.3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей: подтверждение факта обработки персональных данных; правовые основания и цели обработки персональных данных; цели и применяемые оператором способы обработки персональных данных; наименование и место нахождения Оператора, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании законодательства; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством; сроки обработки персональных данных, в том числе сроки их хранения; порядок осуществления субъектом персональных данных прав, предусмотренных законодательством.

1.8.4. Сведения, указанные в п. 1.4.3., предоставляются субъекту персональных данных или его официальному представителю по официальному запросу на имя Оператора.

1.8.5. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

1.8.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

1.8.7. Субъект персональных данных обязан:

- передавать Оператору достоверные, документированные персональные данные, состав которых установлен законодательством;
- своевременно сообщать специалистам Оператора об изменении своих персональных данных.

2. Принципы и цели обработки персональных данных

2.1. Обработка персональных данных в БУЗ ВО «ВОПБ» осуществляется на основе принципов законности и справедливости и ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Персональные данные, цели обработки которых несовместимы между собой, обрабатываются Оператором в различных базах данных; содержание и объем персональных данных соответствуют заявленным целям обработки.

2.3. При обработке персональных данных Оператором обеспечивается их точность, достаточность, а в необходимых случаях актуальность по отношению к целям обработки персональных данных. Работники Оператора обязаны принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

2.4. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется Оператором не дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен действующим законодательством. Обрабатываемые персональные данные подлежат уничтожению или обезличиванию по достижению целей обработки, если иное не предусмотрено действующим законодательством.

2.5. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

2.6. Обработке в БУЗ ВО «ВОПБ» подлежат только те персональные данные, которые отвечают следующим целям обработки:

- оформление и регулирование трудовых отношений в соответствии с требованиями трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права; ведение воинского учета; ведение бухгалтерского учета и формирования налоговой отчетности и отчетности в государственные внебюджетные фонды; обеспечение сохранности архивных документов, в том числе документов по личному составу, в течение сроков их хранения, установленных федеральными законами, иными нормативными правовыми актами Российской Федерации;

- оказание медицинских услуг, в том числе идентификация пациентов (заказчиков), отражение информации в медицинской документации, предоставление установленной законодательством отчетности в отношении оказанных медицинских услуг;

- обеспечение соблюдения законодательства в области здравоохранения;

- обеспечение соблюдения Федерального закона от 2 мая 2006 г. N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

- иные цели, закрепленные в Уставе Оператора.

3. Правовые основания обработки персональных данных

3.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных.

3.2. Обработка персональных данных Оператором ведется на основании:

- Трудового кодекса Российской Федерации;
- Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» и принятых на его основе нормативно-правовых актах, регулирующих отношения, связанные с оказанием медицинских услуг;
- Закона Российской Федерации от 2 июля 1992 г. N 3185-I «О психиатрической помощи и гарантиях прав граждан при ее оказании»;
- Устава бюджетного учреждения здравоохранения Вологодской области «Вологодская областная психиатрическая больница»;
- договоров, заключаемых между Оператором и субъектами персональных данных;
- согласий на обработку персональных данных.

4. Категории субъектов персональных данных, объем и категории обрабатываемых персональных данных

4.1. К категориям субъектов персональных данных, чьи данные обрабатываются Оператором, относятся:

- 4.1.1. работники Оператора, бывшие работники, а также несовершеннолетние дети работников;
- 4.1.2. пациенты (клиенты) и их законные представители;
- 4.1.3. граждане, обратившиеся в БУЗ ВО «ВОПБ» (жалоба, заявление, предложение), в том числе по вопросам предоставления государственных услуг;
- 4.1.4. контрагенты оператора (физические лица).

4.2. В отношении категории субъектов, указанных в пункте 4.1.1. (за исключением несовершеннолетних детей работников) обрабатываются:

- фамилия, имя, отчество, пол, дата и место рождения, гражданство;
- сведения об изменении фамилии, имени, отчества (когда, где и по какой причине);
- данные паспорта гражданина РФ;
- отношение к воинской обязанности и воинское звание;
- сведения о месте регистрации и месте фактического проживания, номер служебного телефона, номер домашнего телефона, номер сотового телефона;
- номер страхового свидетельства обязательного пенсионного страхования (СНИЛС);
- наличие несовершеннолетних детей;
- идентификационный номер налогоплательщика (ИНН);
- сведения о профессиональном образовании (оконченные учебные заведения и год окончания, специальность (направление) и квалификация, наличие ученых степеней, повышение квалификации);

- сведения о наличии судимости (в случаях, установленных законодательством);
- сведения о прохождении аттестации, принятых аттестационными комиссиями решениях, о квалификационной категории;
- сведения о стаже (общий трудовой стаж, стаж государственной (муниципальной) службы, стаж работы по специальности);
- о периодах и местах работы моей трудовой деятельности;
- сведения о выполняемой работе, занимаемой должности, дате принятия на работу, условиях труда, переводах, доплатах, работы на условиях совместительства;
- сведения о результатах специальной оценки условий труда, факторов вредности и т.д.
- сведения о состоянии здоровья, которые относятся к вопросу о возможности выполнения работником трудовых функций;
- сведения об условиях оплаты труда по занимаемой должности;
- реквизиты расчетного (лицевого) счета;
- сведения о режиме труда и отдыха, об отпусках и командировках;
- сведения о награждении государственными и ведомственными наградами, иными наградами;
- фотография с изображением (для получения доступа к наркотическим средствам, психотропным веществам в случаях, установленных законодательством; для размещения на Доску почета БУЗ ВО «ВОПБ»);
- сведения о проведении служебных проверок и наложении дисциплинарных взысканий;
- сведения о временной нетрудоспособности;
- сведения с предыдущих мест работы о доходах;
- иные сведения в рамках регулирования трудовых правоотношений в соответствии с действующим законодательством.

4.3. Персональные данные несовершеннолетних детей работников обрабатываются в объеме, необходимом для предоставления работнику гарантий и компенсаций, предусмотренных действующим законодательством:

- фамилия, имя, отчество;
- дата и место рождения;
- место проживания;
- серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе.

4.4. В отношении пациентов обрабатываются:

- фамилию, имя, отчество,
- пол,
- дату рождения,
- адрес проживания,
- данные паспорта или иного документа, удостоверяющего личность,
- контактный телефон,
- реквизиты полиса ОМС (ДМС),

- страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС),
- данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью,
- биометрические данные,
- иные данные, необходимые для оказания медицинской помощи, в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг.

4.5. В отношении категорий субъектов, указанных в п.п. 4.1.3 - 4.1.4. обрабатываются:

- фамилия, имя, отчество;
- возраст;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный телефон;
- адрес электронной почты;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- иные данные, необходимые для исполнения требований Федерального закона от 2 мая 2006г. N59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

4.6. В отношении законных представителей пациентов или представителей по доверенности обрабатываются:

- фамилия, имя, отчество;
- пол;
- возраст;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный телефон;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- сведения о документе, который подтверждает полномочия представителя.

5. Порядок и условия обработки персональных данных

5.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

5.2. Оператор не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных».

5.3. Форма и содержание письменного согласия субъекта персональных данных определяются Оператором в соответствии с требованиями законодательства.

5.4. Обработка персональных данных осуществляется Оператором следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

5.5. Оператор организует обработку персональных данных в следующем порядке:

5.5.1. назначает ответственного за организацию обработки персональных данных;

5.5.2. устанавливает перечень лиц, имеющих доступ к персональным данным;

5.5.3. утверждает настоящую Политику и локальные акты по вопросам обработки персональных данных;

5.5.4. применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;

5.5.5. осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;

5.5.6. осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;

5.5.7. знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

5.6. Специалисты Оператора, уполномоченные на получение, обработку, хранение, передачу и любое другое использование персональных данных обязаны:

- знать и выполнять требования законодательства в области обеспечения защиты персональных данных;
- хранить в тайне известные им персональные данные, информировать о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей.

5.6.1. Специалистам Оператора, уполномоченным на получение, обработку, хранение, передачу и любое другое использование персональных данных, запрещается:

- использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях – при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;
- передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных средств криптографической защиты информации.

6. Меры, принимаемые для защиты персональных данных

6.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры 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.

6.2. К правовым мерам защиты относятся действующие законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер, Оператор обеспечивает постоянную разъяснительную работу с пользователями и обслуживающим персоналом системы.

6.3. Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых Оператором - обеспечить выполнение настоящей Политики, выделяя необходимые ресурсы и контролируя состояние дел.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры состоят из:

- ограничения доступа в помещения ИСПДн;
- порядка допуска сотрудников к использованию ресурсов ИСПДн Учреждения;
- инструкций пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора ИСПДн);
- инструкции пользователя при возникновении внештатных ситуаций.

6.4. Технические меры защиты персональных данных в информационных системах от несанкционированного (в том числе случайного) доступа, применяемые Оператором включают:

- использование сертифицированных средств антивирусной защиты и средств криптографической защиты информации;
- использование встроенных средств защиты операционных систем и прикладного программного обеспечения;
- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- обнаружение (предотвращение) вторжений;
- обеспечение целостности информационной системы и персональных данных;
- использование программно-аппаратных ключей защиты элементов информационной системы;
- управление конфигурацией информационной системы и системы защиты персональных данных;
- защита каналов связи с центрами обработки данных.
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).
- специалистами Учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. Заключительные положения

7.1. Во исполнение части 2 статьи 18.1. Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» настоящая Политика опубликована на официальном сайте БУЗ ВО «ВОПБ» (<http://вопб.рф>).

7.2. Оператор оставляет за собой право вносить изменения в настоящую Политику (во все ее разделы и преамбулу, а также в наименование).

7.3. Настоящая Политика и законодательством РФ в области персональных данных.