Минздрав России

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Сибирский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО СибГМУ Минздрава России)

УТВЕРЖДАЮ
И.о. ректора

_____ Е.С. Куликов
21.05. _____ 2021

ПОЛИТИКА №42
ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика обработки и защиты персональных данных (далее – политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в области обработки и защиты персональных данных.

1.2. Политика направлена на обеспечение защиты прав и свобод субъектов персональных данных и подлежит размещению на официальном сайте ФГБОУ ВО СибГМУ Минздрава России.

1.3. Политика раскрывает цели, правовые основания обработки персональных данных, категории обрабатываемых персональных данных и источники их получения, основные принципы обработки и меры по обеспечению безопасности персональных данных при их обработке, а также права субъектов персональных данных.

1.4. ФГБОУ ВО СибГМУ Минздрава России имеет право вносить изменения в настоящую политику по мере внесения изменений в нормативные правовые акты в сфере обработки персональных данных в Российской Федерации и/или локальные нормативные акты, регламентирующие организацию обработки и обеспечение безопасности персональных данных.

1.5. Настоящая политика распространяется на деятельность всех структурных подразделений, участвующих в обработке персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Персональные данные –** любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. **Персональные данные, разрешенные субъектом персональных данных для распространения,** – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.3. **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,

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.

2.4. **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.

2.5. **Субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

2.6. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.7. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.8. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.9. **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.

2.10. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

2.11. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

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

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

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных в ФГБОУ ВО СибГМУ Минздрава России осуществляется на законной основе и ограничивается достижением конкретных, заранее определенных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

3.2. При обработке персональных данных обеспечивается их точность, достаточность и актуальность по отношению к целям обработки персональных данных. Неполные или неточные персональные данные удаляются или уточняются.

3.3. Обработка персональных данных работников осуществляется с целью:

- содействия в получении образования, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- предоставления информации в медицинские и страховые организации, а также в банки, которым поручена обработка персональных данных работников в рамках реализации зарплатных программ;
- обеспечения предоставления социального пакета;
- обеспечения безопасности в соответствии с требованиями законодательства об охране труда;
- обеспечения пропускного режима;
- обеспечения сохранности имущества организации.

3.4. Обработка персональных данных обучающихся осуществляется с целью:

- осуществления образовательной деятельности по образовательным программам высшего образования и научной деятельности;
- содействия в трудоустройстве и обучении;
- предоставления информации в государственные органы Российской Федерации в порядке, предусмотренном действующим законодательством РФ;
- предоставления информации в страховые организации, а также в организации, в которых обучающиеся проходят учебную, производственную и преддипломную практики, банки, которым поручена обработка персональных данных обучающихся в рамках реализации стипендиальных программ;
- обеспечения предоставления социальных гарантий, предусмотренных действующим законодательством РФ;
- обеспечения пропускного режима;
- обеспечения сохранности имущества организации.

3.5. Обработка персональных данных пациентов осуществляется с целью:

- оказания качественной медицинской помощи в необходимых объёмах;
- соблюдения требований действующего законодательства Российской Федерации и иных нормативных правовых актов;
- обеспечения контроля объёмов и качества оказанной медицинской помощи;
- ведения учетной статистической документации, используемой в медицинских организациях, в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и иными федеральными законами.

4. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Политика ФГБОУ ВО СибГМУ Минздрава России в области обработки персональных данных определяется следующими основными нормативными правовыми актами.

- Конституцией Российской Федерации
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСТЭК России от 31.05.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- прочими нормативными правовыми актами.

5. КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ И КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. К категориям субъектов персональных данных относятся:

- работники, бывшие работники, кандидаты на замещение вакантных должностей;
- абитуриенты, студенты, бывшие студенты, аспиранты и другие лица, обучающиеся (обучавшиеся) по очной/заочной форме обучения, на бюджетной, коммерческой или иной основе;
- пациенты, бывшие пациенты.

5.2. В состав обрабатываемых в ФГБОУ ВО СибГМУ Минздрава России персональных данных могут входить следующие категории персональных данных: общие, специальные и биометрические.

5.3. К категории общих персональных данных работников, абитуриентов, студентов, аспирантов и других обучающихся, а также пациентов относятся:

- фамилия, имя, отчество;
- паспортные данные;
- СНИЛС;
- ИНН;
- дата и место рождения;
- гражданство;
- адреса регистрации и фактического проживания;
- адрес электронной почты;
- семейное положение;
- место учебы, работы;

- образование;
- профессия и т.д.

5.4. К категории специальных персональных данных, обрабатываемых в ФГБОУ ВО СибГМУ Минздрава России, относится информация, являющаяся врачебной тайной:

- сведения о факте обращения за оказанием медицинской помощи;
- сведения о состоянии здоровья, диагнозе;
- сведения о результатах медицинских исследований;
- иные сведения, полученные при медицинском обследовании и лечении.

5.5. К категории биометрических персональных данных, обрабатываемых в ФГБОУ ВО СибГМУ Минздрава России, относятся данные о физиологических и биологических особенностях работников, абитуриентов, студентов, аспирантов и других обучающихся, а также пациентов.

5.5.1. Биометрические данные работников, абитуриентов, студентов, аспирантов и других обучающихся:

- изображение лица.

5.5.2. Биометрические данные пациентов:

- изображение лица;
- данные геометрии контура кисти руки;
- изображения сосудистого русла;
- изображение радужной оболочки глаза и т.п.

5.6. В соответствии со статьями 10 и 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обработка специальных персональных данных пациентов допускается в случаях, когда:

- пациент дал в письменной форме согласие на обработку персональных данных и согласие на обработку персональных данных, разрешенных для распространения (оформляется отдельно от иных согласий пациента на обработку его персональных данных, молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку его персональных данных, разрешенных для распространения);
- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов пациента либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну.

5.7. В соответствии со статьей 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обработка биометрических персональных данных допускается только при наличии письменного согласия субъекта персональных данных.

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Получение персональных данных.

6.1.1. Получение персональных данных, преимущественно, осуществляется путем предоставления их самим субъектом на основании его письменного согласия, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

6.1.2. В случае недееспособности или смерти субъекта, не достижения им возраста 15 лет или в других случаях, предусмотренных законодательством, согласие на обработку его персональных данных дает в письменной форме его законный представитель.

6.1.3. В обязанности работников, осуществляющих первичный сбор персональных данных пациента, входит получение согласия пациента на обработку его персональных данных и, в случае необходимости, согласия на обработку персональных данных, разрешенных для распространения.

6.2. Обработка персональных данных.

6.2.1. Обработка персональных данных в ФГБОУ ВО СибГМУ Минздрава России осуществляется только с согласия субъекта персональных на обработку своих персональных данных, а также с согласия на обработку персональных данных, разрешенных для распространения.

6.2.2. При обработке персональных данных обеспечивается принятие правовых, организационных и технических мер 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.

6.2.3. Обработка персональных данных в ФГБОУ ВО СибГМУ Минздрава России осуществляется неавтоматизированным и автоматизированным способами.

6.2.4. Доступ работников к обрабатываемым персональным данным осуществляется в строгом соответствии с их должностными обязанностями и требованиями внутренних нормативных документов.

6.2.5. Работники, осуществляющие обработку персональных данных, при трудоустройстве в обязательном порядке подписывают обязательство о неразглашении персональных данных в отделе защиты информации управления информационно-телекоммуникационной инфраструктуры.

6.3. Хранение персональных данных.

6.3.1. Персональные данные хранятся на бумажных носителях и в электронном виде.

6.3.2. Персональные данные на бумажных носителях хранятся в шкафах, запираемых на ключ, либо в запираемых помещениях с ограниченным правом доступа (регистратура, архивы, канцелярия, управление кадрами и т.п.), обеспечивающих защиту от несанкционированного доступа.

6.3.3. Персональные данные в электронном виде хранятся в базах данных информационных системах персональных данных (1С Зарплата и кадры, 1С Университет, 1С Документооборот, Медицинская информационная система Томской области, Единая государственная информационная система в сфере здравоохранения, Информационная система контроля, учета и статистики и т.п.), представляющих собой совокупность персональных данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных и обеспечивать их сохранность и защиту от несанкционированного доступа.

6.3.4. Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках).

6.3.5. Хранение персональных данных осуществляется не дольше, чем этого требуют цели обработки, если иное не предусмотрено действующим законодательством Российской Федерации.

6.3.6. По истечении срока хранения персональные данные должны быть уничтожены в порядке, установленном действующим законодательством Российской Федерации.

6.4. Передача персональных данных.

6.4.1. Под передачей персональных данных понимается передача информации по каналам связи и/или на материальных носителях определенному лицу или определенному кругу лиц.

6.4.2. Передача персональных данных третьим лицам (в том числе трансграничная передача) допускается с письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в иных случаях, установленных действующим законодательством Российской Федерации.

6.4.3. ФГБОУ ВО СибГМУ Минздрава России вправе поручить обработку персональных данных третьим лицам с согласия субъекта персональных данных на основании заключаемых договоров. При этом лица, осуществляющие обработку персональных данных по поручению, обязаны соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством Российской Федерации.

6.5. Распространение персональных данных.

6.5.1. Под распространением персональных данных понимается передача информации по каналам связи и/или на материальных носителях неопределенному кругу лиц.

6.5.2. Распространение персональных данных возможно только с согласия субъекта на обработку его персональных данных, разрешенных для распространения, которое оформляется отдельно от общего согласия на обработку персональных данных. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

6.5.3. Субъект персональных данных вправе обратиться к ФГБОУ ВО СибГМУ Минздрава России, как к оператору персональных данных, с требованием прекратить передачу (распространение) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения. Требование оформляется в виде заявления в свободной форме на имя ректора и подается либо в приемную ректора (Московский тракт, д. 2, главный корпус), либо в приемную главного врача клиник (Московский тракт, д. 2, стр. 21, здание администрации клиник).

6.5.4. Оператор обязан прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных.

6.6. Блокировка, обезличивание, уничтожение персональных данных.

6.6.1. Блокировка персональных данных осуществляется с письменного заявления субъекта персональных данных. Заявление оформляется в свободной форме на имя ректора и подается либо в приемную ректора, либо в приемную главного врача клиник.

6.6.2. Блокировка подразумевает:

- запрет редактирования персональных данных;
- запрет распространения персональных данных любыми средствами;
- изъятие бумажных документов, содержащих персональные данные из внутреннего документооборота и запрет их использования.

6.6.3. Блокировка персональных данных может быть временно снята, если это требуется для соблюдения законодательства Российской Федерации.

6.6.4. Разблокировка персональных данных осуществляется с письменного заявления субъекта персональных данных, оформляемого также в свободной форме на имя ректора и подаваемого либо в приемную ректора, либо в приемную главного врача клиник.

6.6.5. Повторное согласие субъекта на обработку его персональных данных (при необходимости его получения) также влечет разблокирование его персональных данных.

6.6.6. Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к его персональным данным и уничтожение носителей.

6.6.7. Отбор носителей к уничтожению производится экспертной комиссией. Факт уничтожения подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

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

6.6.9. Персональные данные на электронных носителях уничтожаются путем стирания (форматирования) или уничтожения носителя.

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. ФГБОУ ВО СибГМУ Минздрава России при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

7.2. В соответствии с требованиями нормативных документов создана система защиты персональных данных, состоящая из подсистем правовой, организационной и технической защиты.

7.3. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование системы защиты персональных данных.

7.4. Подсистема организационной защиты включает в себя:

- разработку разрешительной системы доступа к персональным данным соответствии с должностными обязанностями работников и требованиями локальных нормативных документов;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных и разработку модели угроз безопасности персональных данных;
- учет машинных носителей персональных данных;
- разработку политики в отношении обработки персональных данных;
- обучение работников, осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, требованиям локальных нормативных документов по вопросам обработки персональных данных в ФГБОУ ВО СибГМУ Минздрава России;
- осуществление внутреннего контроля и аудита.

7.5. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных при обработке в информационных системах персональных данных. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных осуществляется до ввода в эксплуатацию информационной системы персональных данных.

8. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЯЗАННОСТИ ФГБОУ ВО СИБГМУ МИНЗДРАВА РОССИИ КАК ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Субъект персональных данных имеет право:

- получать сведения об обработке его персональных данных у оператора;
- требовать от оператора уточнения, при необходимости, своих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки;
- принимать предусмотренные законом меры по защите своих прав;
- обжаловать действия или бездействие оператора в области обработки его персональных данных путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

8.2. Оператор персональных данных обязан:

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику в отношении обработки персональных данных;
- принимать необходимые правовые, организационные и технические меры для защиты персональных данных от несанкционированного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении персональных данных;
- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных действующему законодательству Российской Федерации и принятым в соответствии с ним нормативным документам;
- предоставлять ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных;
- прекращать неправомерную обработку персональных данных в случае ее выявления, в срок, не превышающий трех рабочих дней с момента такого выявления. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные;
- прекращать обработку и уничтожать персональные данные в случае достижения цели обработки персональных данных в срок, не превышающий тридцати дней с даты достижения цели обработки, если иное не предусмотрено соглашением между оператором и субъектом персональных данных;
- в случае отзыва субъектом согласия на обработку его персональных данных оператор обязан в течение трех рабочих дней прекратить их обработку и, в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить их в срок, не превышающий тридцати дней с

даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных;

- вносить необходимые изменения в персональные данные в срок, не превышающий семи рабочих дней со дня предоставления субъектом или его представителем сведений, подтверждающих, что эти персональные данные являются неполными, неточными или неактуальными. О внесенных изменениях оператор обязан уведомить субъекта или его представителя и принять меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Работники ФГБОУ ВО СибГМУ Минздрава России, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующем законодательством Российской Федерации и внутренними нормативными актами организации.

9.2. Ответственность за организационные мероприятия по защите персональных данных и выполнение требований настоящей политики несут руководители структурных подразделений, в которых обрабатываются персональные данные.

9.3. Ответственность за реализацию технических мероприятий по защите персональных данных, а также контроль за выполнением требований настоящей политики возлагается на отдел защиты информации управления информационно-телекоммуникационной инфраструктуры.

Начальник отдела защиты информации С.П. Клишевич

С.П. Клишевич
901-101 (доб. 2108)
otd.zi@ssmu.ru