

Приложение № 1
к приказу № **175** /Р
от « **16** » **МАР** 20 **15** г.

Министерство здравоохранения Российской Федерации
государственное бюджетное образовательное учреждение высшего профессионального образования
ПЕРВЫЙ МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ
УНИВЕРСИТЕТ имени И.М. СЕЧЕНОВА

ПОЛИТИКА
обработки и обеспечения безопасности персональных данных
в ГБОУ ВПО Первый МГМУ им. И.М. Сеченова Минздрава России

Москва 2015

ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Оператор – Государственное бюджетное образовательное учреждение высшего профессионального образования Первый Московский государственный медицинский университет им. И.М. Сеченова Министерства здравоохранения Российской Федерации (далее – ГБОУ ВПО Первый МГМУ им. И.М. Сеченова Минздрава России);

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;

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;

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

Доступность информации - состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика обработки и обеспечения безопасности персональных данных (далее – Политика) в ГБОУ ВПО Первый МГМУ им. И.М. Сеченова Минздрава России (далее – Оператор) разработана в соответствии с требованиями нормативно-правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой персональных данных (далее – ПДн). Политика определяет принципы сбора, обработки, хранения, передачи и защиты ПДн физических лиц (далее – субъекты ПДн), реализуемые у Оператора.

1.2. Действие настоящей Политики распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПДн, осуществляемых как с использованием средств автоматизации, так и без использования таких средств.

2. НОРМАТИВНЫЕ ДОКУМЕНТЫ, В СООТВЕТСТВИИ С КОТОРЫМИ РАЗРАБОТАНА НАСТОЯЩАЯ ПОЛИТИКА

2.1. Настоящая Политика разработана в соответствии с требованиями следующих нормативно-правовых документов в области защиты ПДн:

- Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановление Правительства РФ от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. ЦЕЛИ ГБОУ ВПО ПЕРВЫЙ МГМУ ИМ. И.М. СЕЧЕНОВА МИНЗДРАВА РОССИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Важнейшими целями Оператора в области защиты персональных данных являются:

- соответствие требованиям законодательства Российской Федерации и договорным обязательствам в части защиты персональных данных при реализации:
 - образовательных программ начального, среднего, высшего, послевузовского и дополнительного профессионального образования;
 - осуществления подготовки, профессиональной переподготовки и (или) повышения квалификации работников высшей квалификации, научных и научно - педагогических работников;
 - выполнения фундаментальных и прикладных научных исследований;
 - организации проведения общественно-значимых мероприятий в сфере образования науки;
 - содействия работникам в трудоустройстве, ведения кадрового учета, оплаты труда, обеспечения личной безопасности, выполнения социальных обязательств;
- обеспечение конфиденциальности, целостности и доступности персональных данных;
- применение адекватных мер по защите от угроз в отношении персональных данных;
- предотвращение и (или) снижение ущерба от реализации угроз в отношении персональных данных.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Принципы обработки персональных данных.

4.1.1. Основные принципы обработки персональных данных Оператора:

- обработка персональных данных должна осуществляться на законной и справедливой основе;

- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.2. Сбор персональных данных.

4.2.1. Сбор, накопление, хранение, изменение, использование и передача ПДн осуществляется при условии наличия согласия субъекта ПДн. Исключение составляют случаи, когда в соответствии с действующим законодательством допускается обработка ПДн без получения согласия субъекта ПДн, а именно:

- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

- обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

- обработка ПДн необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта ПДн;

- обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания ПДн. Исключение составляет обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

- осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн, либо по его просьбе;

- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом

4.3. Хранение персональных данных.

4.3.1. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют соответствующие цели обработки ПДн в

соответствии с законодательством Российской Федерации. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки, или в случае утраты необходимости в достижении этих целей.

4.3.2. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться как на бумажных носителях, так и в электронном виде.

4.3.3. ПДн на бумажных носителях, должны храниться в запираемых шкафах или сейфах структурных подразделений, осуществляющих обработку персональных данных, либо специализированных помещений архива Оператора.

4.3.4. ПДн субъектов в электронном виде обрабатываются в компьютерных сетях Оператора.

4.4. Передача персональных данных третьим лицам.

4.4.1. Оператор обязуется и обязует иных лиц, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законом.

4.5 Трансграничная передача персональных данных.

4.5.1. Трансграничная передача ПДн может осуществляться в соответствии с требованиями законодательства РФ на территорию иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн.

4.5.2. Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- предусмотренных международными договорами Российской Федерации;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект персональных данных;

- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

4.6. Уничтожение персональных данных.

4.6.1. В случае достижения цели обработки ПДн Оператор обязан прекратить обработку ПДн, если иное не предусмотрено договором между Оператором и субъектом персональных данных.

4.6.2. В случае отзыва субъектом ПДн согласия на обработку своих ПДн Оператор обязан прекратить их обработку, если иное не предусмотрено договором между Оператором и субъектом ПДн, либо если Оператор вправе осуществлять обработку ПДн без согласия субъекта ПД на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

4.6.3. В случае выявления неправомерной обработки ПДн Оператор должен предпринять меры по уничтожению этих ПДн в срок, не превышающий семи рабочих дней со дня выявления неправомерной обработки ПДн.

4.6.4. В случае отсутствия возможности уничтожения ПДн в течение указанного срока, Оператору необходимо осуществить блокирование таких ПДн и обеспечить уничтожение ПДн в срок, не превышающий 6 месяцев со дня выявления неправомерной обработки ПДн, если иной срок не установлен федеральным законодательством.

4.6.5. В случае если уничтожение ПДн было произведено по результатам обработки обращения субъекта ПДн и (или) запроса уполномоченного органа по защите прав субъектов ПДн, о предпринятых действиях Оператор обязан уведомить субъекта ПД и (или) уполномоченный орган по защите прав субъектов ПДн.

4.6.6. ПДн на бумажных носителях необходимо уничтожать с помощью средств, гарантирующих невозможность восстановления носителя ПДн.

4.6.7. Уничтожение информации с машиночитаемых носителей ПДн, пришедших в негодность или утративших практическую ценность, должно производиться способом, исключающим возможность использования и восстановления информации.

4.7. Защита персональных данных.

4.7.1. При обработке ПДн Оператору необходимо принимать правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования,

предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

4.7.2. Обеспечение безопасности ПДн должно достигаться, в частности:

- определением угроз безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн);
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием необходимых мер;
- установлением правил доступа к ПДн, обрабатываемых в ИСПДн, а также обеспечением регистрации доступа к ПДн в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

5 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1. Общие положения.

5.1.1. Оператору необходимо обеспечивать конфиденциальность ПДн, то есть не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

5.2 Организация внутреннего доступа сотрудников к персональным данным.

5.2.1. В рамках данной Политики под внутренним доступом понимается доступ к ПДн, предоставляемый работникам Оператора, допущенных к обработке персональных данных.

5.2.2. Доступ к ПДн необходимо предоставлять только тем работникам Оператора, которым ПДн необходимы для исполнения их непосредственных должностных обязанностей.

5.2.3. Допуск работников Оператора к обработке ПДн требуется осуществлять на основании утвержденного Перечня работников структурных подразделений, допущенных к работе с ПДн, обрабатываемыми у Оператора.

5.2.4. Работник Оператора должен допускаться к обработке ПДн только после ознакомления с внутренними нормативными документами Оператора, регламентирующими обработку ПДн, под роспись, а также после подписания Обязательства о неразглашении персональных данных.

5.3. Организация доступа субъектов персональных данных к своим персональным данным.

5.3.1. Оператор обязан обеспечивать доступ субъектов ПДн к принадлежащим им ПДн. Для получения такого доступа субъекту ПДн необходимо направить Оператору запрос через Канцелярию (письменный запрос или запрос в форме электронного документа, подписанный электронной подписью). Оператор осуществляет предоставление ПДн обратившегося субъекта в доступной для субъекта форме, и с обеспечением отсутствия в них ПДн, относящихся к другим субъектам.

5.3.2. В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» субъект ПД имеет право:

1. Получить сведения касающиеся обработки ПДн Оператором, а именно:
 - подтверждение факта обработки персональных данных субъекта ПДн;
 - правовые основания и цели обработки персональных данных субъекта ПДн;
 - цели и применяемые способы обработки персональных данных субъекта ПДн;
 - наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным субъекта ПДн или которым могут быть раскрыты персональные данные субъекта ПДн на основании договора с оператором или на основании федерального закона;
 - обрабатываемые персональные данные, относящиеся к субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
 - сроки обработки персональных данных субъекта ПДн, в том числе сроки их хранения;
 - порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
 - информацию об осуществленной или о предполагаемой трансграничной передаче данных субъекта ПДн;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных субъекта ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу.

2. Потребовать 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.

3. Заявить возражение против принятия в отношении себя решений, порождающих юридические последствия на основе исключительно автоматизированной обработки ПДн.

4. Потребовать исключения своих ПДн из общедоступных источников персональных данных.

5. Отозвать согласие на обработку ПДн в предусмотренных законом «О персональных данных» случаях.

5.3.3. Право субъекта ПДн на доступ к своим данным ограничивается в случае, если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса,

защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

6. ОТВЕТСТВЕННОСТЬ

6.1. Оператор несет ответственность за защиту ПДн субъектов ПДн, обязуется не разглашать конфиденциальную информацию и не использовать ее, кроме как в целях исполнения договорных обязательств при реализации образовательных программ, осуществления профессиональной подготовки субъектов ПДн и других целей, не противоречащих законодательству Российской Федерации.

6.2. При нарушении у Оператора норм, регулирующих получение, обработку и защиту ПДн, субъекты ПДн несут дисциплинарную, административную, гражданско-правовую, уголовную и иную ответственность в соответствии с законодательством Российской Федерации.

6.3. За предоставление неполных, неточных или неактуальных сведений субъектом ПДн Оператор ответственности не несет.

