Приложение №1
Приказа Министерства здравоохранения
Республики Мордовия
от «12» 11 2021 г. № 2101

Политика в отношении обработки персональных данных в государственной информационной системе в сфере здравоохранения Республики Мордовия

Министерства здравоохранения Республики Мордовия

г. Саранск
2021 год

1. Общие положения

Настоящая «Политика в отношении обработки персональных данных…» (далее – Политика), разработана в целях обеспечения безопасности персональных данных, является официальным документом.

Обеспечение конфиденциальности и безопасности обработки персональных данных в Министерстве здравоохранения Республики Мордовия является одной из приоритетных задач организации.

В Министерстве здравоохранения Республики Мордовия для данных целей введен в действие комплект организационно-распорядительной документации, обязательный к исполнению всеми сотрудниками Министерства здравоохранения Республики Мордовия, допущенными к обработке персональных данных.

Обработка, хранение и обеспечение конфиденциальности и безопасности персональных данных осуществляется в соответствии с действующим законодательством РФ в сфере защиты персональных данных, и в соответствии с локальными актами Министерства здравоохранения Республики Мордовия.

Настоящая Политика определяет принципы, порядок и условия обработки персональных данных работников, пациентов, соискателей и контрагентов Министерства здравоохранения Республики Мордовия и иных лиц, чьи персональные данные обрабатываются в Министерстве здравоохранения Республики Мордовия, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц Министерства здравоохранения Республики Мордовия, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Поскольку к настоящей Политике в соответствии с ч. 2 ст. 18.1 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» необходимо обеспечить неограниченный доступ, в ней **не публикуется** детальная информация о принятых мерах по защите персональных данных в Министерстве здравоохранения Республики Мордовия, а также иная информация, использование которой неограниченным кругом лиц может нанести ущерб Министерству здравоохранения Республики Мордовия или субъектам персональных данных.

В Политике определены требования к персоналу Министерства здравоохранения Республики Мордовия, степень ответственности персонала, структура и необходимый уровень защищенности информационных систем, предназначенных для обработки персональных данных, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных, в том числе в информационных систем персональных данных Министерства здравоохранения Республики Мордовия.

Целью настоящей Политики является обеспечение безопасности объектов защиты Министерства здравоохранения Республики Мордовия от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций, или уничтожения данных.

Состав персональных данных, подлежащих защите в Министерстве здравоохранения Республики Мордовия, представлен в утвержденных в Министерстве здравоохранения Республики Мордовия перечнях персональных данных, разрешенных для обработки, в том числе, в информационных системах персональных данных Министерства здравоохранения Республики Мордовия.

Состав информационных систем персональных данных Министерства здравоохранения Республики Мордовия, представлен в утвержденном перечне информационных систем персональных данных в Министерстве здравоохранения Республики Мордовия.

2. Термины и определения

В настоящем документе используются следующие термины и их определения.

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

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Доступ к информации – возможность получения информации и ее использования.

Доступность персональных данных – свойство безопасности персональных данных, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом, затрагивающих права и свободы субъекта персональных данных или других лиц.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов, персональных данных, осуществляются при непосредственном участии человека.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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

Целостность персональных данных – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Общие требования по защите персональных данных

Под угрозой безопасности или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена за счет средств Министерства здравоохранения Республики Мордовия в порядке, установленном федеральным законом.

«Внутренняя защита»

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключается бесконтрольное использование защищаемой информации;
- знание работниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

– определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

– организация порядка уничтожения информации;

– своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

– воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

– не допускается выдача личных дел сотрудников на рабочие места сотрудников. Личные дела могут выдаваться на рабочие места только руководителю, работникам кадрового подразделения и, в исключительных случаях, по письменному разрешению руководителя, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

Защита персональных данных сотрудника на электронных носителях

Все папки в электронном виде, содержащие персональные данные, должны быть защищены паролем, который сообщается руководителю кадрового подразделения и начальнику информационно-аналитического отдела.

«Внешняя защита»

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в кадровом подразделении.

Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

– установление границ контролируемой зоны;

– пропускной режим в организации;

– учет и порядок выдачи удостоверений;

– технические средства охраны, сигнализации;

– порядок охраны территории, зданий, помещений, транспортных средств;

– требования к защите информации при интервьюировании и собеседованиях.

Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

По возможности, персональные данные обезличиваются.

Кроме мер защиты персональных данных, установленных законодательством, работодатель, работники и их представители могут вырабатывать совместные меры защиты персональных данных.

Требования настоящего Политики распространяются на всех сотрудников Министерства здравоохранения Республики Мордовия (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

4. Понятие и состав персональных данных

Сведениями, составляющими персональные данные, в Министерстве здравоохранения Республики Мордовия является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Перечень персональных данных, подлежащих защите в Министерстве здравоохранения Республики Мордовия определятся целями их обработки, Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», Федеральным законом «Об основах охраны здоровья граждан в Российской Федерации» от 21 ноября 2011 года №323-ФЗ, Трудовым кодексом РФ и иными нормативно-правовыми актами.

5. Система защиты персональных данных в информационных системах

Система защиты персональных данных в Министерстве здравоохранения Республики Мордовия строится на основании:

- перечня персональных данных, подлежащих защите;
- класса защищенности информационных систем;
- акта определения уровня защищенности персональных данных в информационных системах;
- модели угроз безопасности персональных данных;
- руководящих документов ФСТЭК России и ФСБ России.

На основании данных документов определяется необходимый уровень защищенности персональных данных каждой информационной системы персональных данных Министерства здравоохранения Республики Мордовия.

На основании анализа актуальных угроз безопасности персональных данных, описанных в Модели угроз информационной системы персональных данных Министерства здравоохранения Республики Мордовия, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности персональных данных.

В зависимости от уровня защищенности информационной системы персональных данных и актуальных угроз, система защиты персональных данных может включать в себя сертифицированные по требованиям безопасности информации средств защиты информации от несанкционированного доступа, антивирусные средства защиты, средства межсетевого экранирования, средства обнаружения вторжений, средства

криптографической защиты информации при передаче защищаемой информации по каналам связи.

6. Субъекты доступа к персональным данным в информационных систем персональных данных

В Политике определены основные категории субъектов доступа к персональным данным в информационных систем персональных данных. На основании этих категорий должны быть определены их полномочия доступа к информационным системам персональных данных.

Субъектами доступа к персональным данным в информационных систем персональных данных являются:

- медицинские информационные системы;
- операторы системы диспетчеризации скорой помощи;
- службы обработки вызовов и телефонии;
- разработчики информационных систем;
- администраторы информационной безопасности и системные;
- администраторы ГАУ Республики Мордовия «Госинформ».

Должностные обязанности субъектов доступа к персональным данным регламентированы утвержденным комплектом организационно-распорядительной документации.

7. Требования к персоналу

Сотрудники Министерства здравоохранения Республики Мордовия должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования персональных данных.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с персональными данными, элементами информационных систем персональных данных и системы защиты персональных данных.

Сотрудники Министерства здравоохранения Республики Мордовия, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Министерства здравоохранения Республики Мордовия должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей.

Сотрудники Министерства здравоохранения Республики Мордовия должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с персональных данных, третьим лицам.

При работе с персональными данными в информационных системах сотрудники Министерства здравоохранения Республики Мордовия обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с экранов мониторов.

Сотрудники Министерства здравоохранения Республики Мордовия должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности персональных данных.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационных систем персональных данных, могущих повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

8. Ответственность сотрудников Министерства здравоохранения Республики Мордовия

В соответствии со ст. 24 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» лица, виновные в нарушении требований по обеспечению безопасности персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

Ответственность за нарушение требований по обеспечению безопасности персональных данных должна быть отражена в должностных инструкциях сотрудников Министерства здравоохранения Республики Мордовия, осуществляющих обработку персональных данных, в том числе в информационных системах персональных данных Министерства здравоохранения Республики Мордовия.

9. Права и обязанности

Министерство здравоохранения Республики Мордовия как оператор персональных данных вправе:

– отстаивать свои интересы в суде;

– предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

– отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

– использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством.

Министерство здравоохранения Республики Мордовия как оператор персональных данных обязан:

– обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законом;

– внести необходимые изменения, уничтожить или блокировать персональные данные в случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных, а также уведомить о своих действиях субъекта персональных данных;

– выполнять требования законодательства Российской Федерации.

Субъект персональных данных имеет право:

– требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

– требовать перечень своих персональных данных, обрабатываемых Министерством здравоохранения Республики Мордовия и источник их получения;

– получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

– требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

Субъект персональных данных обязан:

– передавать достоверные, необходимые для достижения целей обработки, персональные данные, а также подтверждать достоверность персональных данных предъявлением оригиналов документов;

– в случае изменения персональных данных, необходимых для достижения целей обработки, сообщить Министерству здравоохранения Республики Мордовия уточненные персональные данные и подтвердить изменения оригиналами документов;

– выполнять требования законодательства Российской Федерации.

10. Заключительные положения

К настоящей Политике обеспечивается неограниченный доступ.

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

Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных Министерства здравоохранения Республики Мордовия.