Приложение № 3

УТВЕРЖДЕНО
приказом ОГКУЗ «МИАЦ»
от «28» 01 22г. № 4-ОД

Политика ОГКУЗ «МИАЦ» в отношении организации и обеспечения безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика Областного государственного казенного учреждения здравоохранения «Медицинский информационно-аналитический центр» (далее - Оператор) в отношении организации обработки и обеспечения безопасности (далее - Политика) характеризуется следующими признаками:

1.1.1. Разработана в целях реализации требований законодательства Российской Федерации в области обработки и защиты персональных данных субъектов.

1.1.2. Раскрывает способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

1.1.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке и защите персональных данных.

1.2. Оператор до начала обработки персональных осуществил уведомление уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. Оператор добросовестно и в соответствующий срок осуществляет актуализацию сведений, указанных в уведомлении.

1.3. Основные понятия

1.3.1. Для целей Политики используются следующие понятия:

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

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 «О персональных данных»;

субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;
оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

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;

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

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

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Основанием обработки персональных данных Оператора являются следующие нормативные акты и документы:

2.1.1. Конституция Российской Федерации;

2.1.2. Трудовой кодекс Российской Федерации;

2.1.3. Налоговый кодекс Российской Федерации;

2.1.4. Федеральный закон №152-ФЗ от 27.07.2006 «О персональных данных»;

2.1.5. Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»;

2.1.6. Федеральный закон от 29 июля 2017 г. №242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»;

2.1.7. Федеральный закон от 30.12.2012 г. № 329-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения учета изменений состояния здоровья отдельных категорий граждан, подвергшихся радиационному воздействию»;

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

2.1.9. Федеральный закон №187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»;

2.1.10. Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военнослужащих»;

2.1.11. Федеральный закон от 28 июня 1991 г. № 1499-1 «О медицинском страховании граждан в Российской Федерации»;

2.1.12. Федеральный закон Российской Федерации от 30 марта 1999 г. № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»;

2.1.13. Федеральный закон Российской Федерации от 17 сентября 1998 г. № 157-ФЗ «Об иммунопрофилактике инфекционных болезней»;

2.1.14. Федеральный закон Российской Федерации от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

2.1.15. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

2.1.16. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

2.1.17. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

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

2.1.19. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

2.1.20. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2.1.21. Постановление Правительства РФ от 23.07.2013 г. № 625 «О порядке формирования и ведения Национального радиационно-эпидемиологического регистра»;

2.1.22. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по

обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

2.1.23. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

2.1.24. Приказ Минздрава России от 23.03.2015 г. № 134н «О формах Национального радиационно-эпидемиологического регистра, порядке верификации информации, включенной в единую федеральную базу данных Национального радиационно-эпидемиологического регистра, а также доступа к ней»;

2.1.25. Закон Еврейской автономной области от 01.07.2015 № 737-ОЗ «О государственных информационных системах Еврейской автономной области»;

2.1.26. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15 февраля 2008 г.);

2.1.27. Устав ОГКУЗ «МИАЦ»;

2.1.28. Иные локальные акты Оператора в сфере обработки и защиты персональных данных.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных осуществляется Оператором в следующих целях:

3.1.1. Выполнение требований законодательства Российской Федерации в сфере здравоохранения; оказание медицинской помощи населению, обеспечение соблюдения законов и иных нормативных правовых актов в сфере здравоохранения:

– формирование единой государственной информационной системы здравоохранения Еврейской автономной области путем организации на базе современных компьютерных технологий отраслевой системы сбора информации;

– формирование базы данных Национального радиационно-эпидемиологического регистра.

3.1.2. Выполнение требований трудового законодательства Российской Федерации:

3.1.2.1. оформление трудовых отношений;

– ведение бухгалтерского и кадрового учета;

– оформление договорных отношений в соответствии с законодательством Российской Федерации.

4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных осуществляется на законной и справедливой основе;

4.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

4.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

4.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки;

4.5. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки и не являются избыточными по отношению к заявленным целям их обработки;

4.6. При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Принимаются необходимые меры по удалению или уточнению неполных или неточных данных;

4.7. Хранение персональных данных осуществляется 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 по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, подлежат уничтожению либо обезличиванию.

4.8. Обработка персональных данных Оператором включает в себя:

- Сбор;
- Запись;
- Систематизация;
- Накопление;
- Хранение;

– уточнение (обновление, изменение);
– извлечение;
– использование;
– передача (распространение, предоставление, доступ);
– блокирование персональных данных.

4.9. Оператор установил следующие условия прекращения обработки персональных данных:

– достижение целей обработки персональных данных и максимальных сроков хранения;
– утрата необходимости в достижении целей обработки персональных данных;
– предоставление субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
– невозможность обеспечения правомерности обработки персональных данных;
– отзыв субъектом персональных данных согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных;
– истечение сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка персональных данных.

4.10. Оператор осуществляет обработку специальных категорий персональных данных (сведения о состоянии здоровья) во исполнение требований действующего трудового законодательства Российской Федерации и действующего законодательства Российской Федерации в сфере здравоохранения.

4.11. Оператор осуществляет обработку персональных данных с использованием средств автоматизации и без использования средств автоматизации.

5. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В соответствии с целями обработки персональных данных, указанными в п. 3 настоящей Политики, Оператором осуществляется

обработка следующих категорий субъектов персональных данных:

– Работники, состоящие в трудовых отношения с ОГКУЗ «МИАЦ»;

– Граждане, подвергшиеся воздействию радиации вследствие катастрофы на Чернобыльской АЭС, других радиационных аварий, ядерных испытаний и иных радиационных катастроф и инцидентов;

– Сотрудники и пациенты лечебно-профилактических учреждений Еврейской автономной области;

5.2. В соответствии с целями обработки персональных данных, указанными в п. 3 настоящей Политики, Оператором осуществляется обработка персональных данных в соответствии с Приложением № 14 «Перечень персональных данных, обрабатываемых в ОГКУЗ «МИАЦ».

6. МЕРЫ ПО НАДЛЕЖАЩЕЙ ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Оператор 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. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

6.1.1. Назначением ответственного лица за организацию обработки персональных данных.

6.1.2. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных.

6.1.3. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

6.1.4. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.

6.1.5. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

6.1.6. Учетом машинных носителей персональных данных.

6.1.7. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

6.1.8. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

6.1.9. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

6.1.10. Контролем над принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

6.2. Обязанности работников Оператора, осуществляющих обработку и защиту персональных данных, а также их ответственность, определяются в соответствующих должностных инструкциях Оператора.

7. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.

7.2. Субъект персональных данных вправе требовать от Оператора уточнения этих 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, а также принимать предусмотренные законом меры по защите своих прав.

7.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

7.4. Для реализации и защиты своих прав и законных интересов субъект персональных данных имеет право обратиться к Оператору. Оператор рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

7.5. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите

прав субъектов персональных данных.

7.6. 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.

8. ЛИЦО, ОТВЕТСТВЕННОЕ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Учреждение назначает лицо, ответственное за организацию обработки персональных данных.

8.2. Лицо, ответственное за организацию обработки персональных данных, в частности, выполняет следующие функции:

8.2.1. осуществляет внутренний контроль за соблюдением Учреждением и работниками Учреждения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

8.3. доводит до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

9. ОТВЕТСТВЕННОСТЬ

9.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

9.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.