

Приложение 1
к приказу КГБУЗ «Медицинский
центр – управляющая компания
Алтайского медицинского кластера»
от 16.05.2016 № 19

ПОЛИТИКА в отношении обработки персональных данных

Общие положения

КГБУЗ «Медицинский центр – управляющая компания Алтайского медицинского кластера» (далее - Оператор) осуществляет свою деятельность в соответствии с действующим законодательством Российской Федерации по направлениям, обозначенным в полученных лицензиях на осуществление медицинской деятельности. Оказание медицинских услуг предполагает обработку и хранение персональных данных пациентов и работников. В соответствии с действующим законодательством наша организация выполнила комплекс технических и организационных мероприятий для обеспечения безопасности обрабатываемых и хранимых персональных данных.

Одна из приоритетных задач в работе Оператора - соблюдение действующего законодательства Российской Федерации в области информационной безопасности, а также требований федерального закона от 27.06.2006 №152-ФЗ «О персональных данных», основной целью которого является обеспечение 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.

Правовые основания обработки персональных данных

Политика Оператора в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами Российской Федерации:

- 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»,
- Федеральный закон от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»,
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

- Приказ 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».

Цели обработки персональных данных

- Бухгалтерский учет и контроль финансово-хозяйственной деятельности Оператора и исполнения финансовых обязательств по заключенным договорам.

- Поддержание контактов с законными представителями субъекта персональных данных.

- Формирование отчетов.

- Ведение кадровой работы.

- Иные задачи, необходимые для повышения качества и эффективности деятельности Оператора.

- Иные задачи, связанные с заключенными договорами и обязательствами.

Принципы обработки персональных данных

При обработке персональных данных Оператор придерживается следующих принципов:

- соблюдение законности получения, обработки, хранения, а также других действий с персональными данными;

- обработка персональных данных исключительно с целью исполнения своих обязательств по договору оказания услуг, а также по трудовому договору;

- сбор только тех персональных данных, которые минимально необходимы для достижения заявленных целей обработки;

- выполнение мер по обеспечению безопасности персональных данных при их обработке и хранении;

- соблюдение прав субъекта персональных данных на доступ к его персональным данным;

- соответствие сроков хранения персональных данных заявленным целям обработки.

Конфиденциальность персональных данных

Работники Оператора и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Состав персональных данных

В состав обрабатываемых Оператором персональных данных могут входить:

- фамилия, имя, отчество;

- пол;
- дата рождения или возраст;
- паспортные данные;
- адрес проживания;
- номер телефона, факса, адрес электронной почты (по желанию);
- данные о воинском учете;
- информация о трудовой деятельности до приема на работу;
- информация об образовании;
- информация о трудовом стаже;
- оклад;
- семейное положение и состав семьи;
- ИНН;
- Информация о знании иностранных языков;
- информация о состоянии здоровья;
- другая информация, необходимая для правильного проведения и интерпретации медицинских исследований;
- результаты выполненных медицинских исследований;
- другая информация, необходимая для выполнения обязательств организации в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, законодательством об обязательных видах страхования, со страховым законодательством, приказами Министерства Здравоохранения РФ, приказами ФСБ.

Сбор (получение) персональных данных

Персональные данные субъектов Оператор получает только лично от субъекта или от его законного представителя. Персональные данные субъекта могут быть получены с его слов и не проверяются. Субъект дает письменное согласие на обработку персональных данных.

Обработка персональных данных

Обработка персональных данных Оператором происходит как неавтоматизированным, так и автоматизированным способом.

К обработке персональных данных допускаются только работники прошедшие определенную процедуру допуска, к которой относятся:

- ознакомление работника с локальными нормативными актами организации (положения, инструкции и т.д.), строго регламентирующими порядок и процедуру работы с персональными данными;
- взятие с работника обязательства о неразглашении в отношении персональных данных при работе с ними;
- получение работником и использование в работе индивидуальных атрибутов доступа к информационным системам персональных данных. При этом каждому работнику выдаются минимально необходимые для исполнения трудовых обязанностей права на доступ в информационные системы.

Работники, имеющие доступ к персональным данным, получают только ту информацию, которая необходима им для выполнения конкретных трудовых функций.

Хранение персональных данных

Персональные данные субъектов хранятся в бумажном (копии документов) и электронном виде. В электронном виде персональные данные субъектов хранятся в информационных системах персональных данных. При хранении персональных данных соблюдаются организационные и технические меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним. К ним относятся:

- назначение работника ответственного за тот или иной способ хранения персональных данных;
- ограничение физического доступа к местам хранения и носителям;
- учет всех информационных систем.

Передача персональных данных третьим лицам

Передача персональных данных третьим лицам возможна в исключительных случаях только с согласия субъекта и только с целью исполнения обязанностей перед субъектом персональных данных в рамках оказания услуг, кроме случаев, когда такая обязанность у Оператора наступает в результате требований федерального законодательства или при поступлении запроса от уполномоченных государственных органов. В данном случае Оператор ограничивает передачу персональных данных запрошенным объемом.

Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача персональных данных без его согласия допускается действующим законодательством РФ. В качестве такого разрешения могут выступать:

- нотариально заверенная доверенность;
- собственноручно написанная субъектом доверенность в присутствии уполномоченного работника Оператора и им заверенная.

Сведения о третьих лицах,

участвующих в обработке персональных данных

В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

- Федеральной налоговой службе,
- Пенсионному фонду Российской Федерации,
- Фонду медицинского страхования Алтайского края,
- Военным комиссариатам Алтайского края.

Меры по обеспечению безопасности персональных данных

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:

- Назначением ответственных за организацию обработки персональных данных,

- Осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам,

- 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, и (или) обучением указанных работников,

- Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных,

- 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,

- Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер,

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

- 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,

- Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных,

- Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

Права субъекта персональных данных

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- применяемые способы обработки персональных данных;
- сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных своих прав;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

Соответствующая информация предоставляется субъекту персональных данных или его представителю при обращении либо при получении запроса от субъекта персональных данных или его законного представителя. Запрос должен быть составлен в соответствии с порядком обработки обращений субъектов персональных данных по вопросам обработки их персональных данных.

Порядок обработки обращений субъектов персональных данных по вопросам обработки персональных данных

В случае обращения либо получения Оператором запроса субъекта персональных данных (или его законного представителя) по вопросам обработки персональных данных, такой запрос передается лицу, ответственному за организацию обработки персональных данных.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Оператор отвечает на полученный запрос в течение 30 (тридцати) календарных дней со дня получения запроса.

Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.

В случае, если сведения, а также обрабатываемые персональные данные, были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно к Оператору или направить повторный запрос в целях получения сведений, касающихся его персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного выше, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, касающимися его персональных данных, должен содержать обоснование направления повторного запроса.

Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным в данном Порядком. Такой отказ должен предоставляться Оператором субъекту персональных данных с обоснованием причины отказа.

Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

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