

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ АЛТАЙСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ
«АЛТАЙСКИЙ КРАЕВОЙ ГОСПИТАЛЬ ДЛЯ ВЕТЕРАНОВ ВОЙН»
(КГБУЗ «АКГВВ»)

П Р И К А З

07 июня 2017 г.

№ 41

г. Барнаул

Об утверждении Политики
в отношении обработки персональных данных
в КГБУЗ «Алтайский краевой госпиталь для ветеранов войн»

Во исполнение требований Федерального закона от 27.07.2006 № 152 «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также иных нормативных документов по защите информации, п р и к а з ы в а ю:

1. Утвердить и ввести в действие Политику в отношении обработки персональных данных КГБУЗ «АКГВВ» (Приложение № 1).
2. Ответственным за обработку персональных данных в структурных подразделениях ознакомить работников Госпиталя под роспись в «Журнале регистрации проведения инструктажа по информационной безопасности» с «Политикой в отношении обработки персональных данных в КГБУЗ «Алтайский краевой госпиталь для ветеранов войн».
3. Начальнику отдела кадров Лицкой Е.Г. осуществлять ознакомление вновь принимаемых сотрудников с «Политикой в отношении обработки персональных данных КГБУЗ «Алтайский краевой госпиталь для ветеранов войн».
4. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник КГБУЗ «АКГВВ»

О.А. Зубова

Приложение № 1
УТВЕРЖДЕНА
приказом начальника КГБУЗ «АКГВВ»
от 07.06.2017 № 71

ПОЛИТИКА
в отношении обработки персональных данных
КГБУЗ «Алтайский краевой госпиталь для ветеранов войн»

1. Общие положения

КГБУЗ «Алтайский краевой госпиталь для ветеранов войн» (далее - Учреждение) 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 организации - соблюдение действующего законодательства Российской Федерации в области информационной безопасности, а так же требований федерального закона от 27.06.2006 года №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.

2. Правовые основания обработки персональных данных

Политика Учреждения в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Налоговым 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 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

Федеральным законом от 24.07.2009 N212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»;

Федеральным законом от 01.04.1996 N 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

Федеральным законом от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»,

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

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»;

Лицензиями на осуществление медицинской деятельности.

3. Задачи решаемые при обработке персональных данных.

Обработка персональных данных субъектов персональных данных осуществляется при решении следующих задач:

оказании медицинской помощи ветеранам войн и лицам, приравненным к ним по льготам (проведение лечебно-профилактических мероприятий, ведение медицинской документации, формирование отчетов по медицинской деятельности Учреждения);

ведении кадровой работы;

начислении заработной платы, учете отчислений и уплаты налогов и иных выплат в фонды;

ведении бухгалтерского учета и контроле финансово-хозяйственной деятельности, исполнении финансовых обязательств по заключенным договорам;

осуществлении расчетов с ТФОМС и страховыми медицинскими организациями за оказанные медицинские услуги застрахованным;

поддержании контактов с законными представителями субъекта персональных данных;

иные задачи, необходимые для повышения качества и эффективности деятельности Учреждения.

4. Принципы обработки персональных данных

При обработке персональных данных Учреждение 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 оказанию медицинской помощи согласно полученных лицензий на осуществление медицинской деятельности, 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.

5. Конфиденциальность персональных данных

Работники Учреждения 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. Работники Учреждения дают письменное обязательство о неразглашении персональных данных.

6. Состав персональных данных

В состав обрабатываемых в Учреждении персональных данных субъектов могут входить:

фамилия, имя, отчество;

пол;

дата рождения или возраст;

паспортные данные;

адрес проживания;

номер телефона, факса, адрес электронной почты (по желанию);

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.

7. Сбор (получение) персональных данных

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

Учреждение осуществляет обработку данных о состоянии здоровья пациентов в целях оказания медицинских услуг, установления медицинского диагноза при этом обработка персональных данных осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Учреждение осуществляет обработку данных о состоянии здоровья работников организации в соответствии с законодательством Российской Федерации.

8. Обработка персональных данных

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

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

ознакомление работника с локальными нормативными актами Учреждения (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 Учреждения, содержащим в себе персональные данные. 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.

9. Хранение персональных данных

Персональные данные субъектов хранятся в бумажном и электронном виде. В электронном виде персональные данные субъектов хранятся в информационных системах персональных данных Учреждения, а также в архивных копиях баз данных этих систем. Порядок архивирования и сроки хранения архивных копий баз данных информационных систем персональных

данных Учреждения определены в инструкции о резервном копировании, которая является обязательной для исполнения администраторами соответствующей системы.

При хранении персональных данных субъектов 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 и материальных носителей, а также архивных копий;

установка охранной сигнализации и видеонаблюдения;

защита локальной сети с помощью межсетевое экранирования;

защита информации на компьютерах системой паролей;

установка антивирусного программного обеспечение.

10. 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 Учреждения наступает в результате требований федерального законодательства или при поступлении запроса от уполномоченных государственных органов. В данном случае Учреждение ограничивает передачу персональных данных запрошенным объемом.

Персональные данные пациента (в том числе результаты исследований) могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента, за исключением случаев, когда передача персональных данных без его согласия допускается действующим законодательством Российской Федерации.

11. Сведения о третьих лицах, участвующих в обработке персональных данных

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

органам Федеральной налоговой службе;

органам Пенсионного фонда Российской Федерации;

Территориальному фонду медицинского страхования Алтайского края;

Страховым медицинским организациям, с которыми заключены соответствующие договора и соглашения.

12. Меры по обеспечению безопасности персональных данных при их обработке

Учреждение 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 Учреждения, 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;

учетом материальных носителей 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.

13. 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 (за исключением работников организации), 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 фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению организации, если обработка поручена или будет поручена такому лицу.

Соответствующая информация предоставляется субъекту персональных данных или его представителю при обращении либо при получении запроса 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.

14. Порядок обработки обращений субъектов персональных данных по вопросам обработки их персональных данных

В случае обращения либо получения Учреждением 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 Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, 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.

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

Сведения предоставляются субъекту персональных данных Учреждением 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 Учреждением 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 в Учреждение 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 в Учреждение 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.

Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным в данной Политике. Такой отказ должен предоставляться Учреждением субъекту персональных данных письменно с обоснованием причины отказа.

Субъект персональных данных вправе требовать от Учреждения 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 Учреждение 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 Учреждения в уполномоченный орган по защите прав субъектов

персональных данных или в судебном порядке.

15. Заключительные положения

Настоящая Политика обработки персональных данных действует в отношении всей информации, которую Учреждение может получить о пользователе во время использования им сервисов официального сайта Учреждения. Использование сервисов сайта означает безоговорочное согласие пользователя с настоящей Политикой и указанными в ней условиями обработки его персональной информации; в случае несогласия с этими условиями пользователь должен воздержаться от использования сервисов сайта Учреждения.