ООО «КЛИНИКА «ВАШ ДОКТОР»
369000, КЧР, г. Черкесск, ул. Ставропольская, 40-а, кабинет №5
ОГРН: 1150917000574, ИНН: 0917026673, КПП: 091701001, ОКПО: 91409367, ЛО-09-01-000504

ПРИКАЗ

Об обеспечении защиты персональных данных

№1-4/2016 от 04.04.2016

В целях исполнение требований Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных» и обеспечения режима конфиденциальности и защиты при работе с материальными носителями персональных данных и в соответствии с требованиями положения об особенностях обработки персональных данных субъектов, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства РФ от 15 сентября 2008 года N 687, приказываю:

1 Утвердить «Политика обработки и защиты персональных данных общества с ограниченной ответственностью «КЛИНИКА «ВАШ ДОКТОР» в соответствии с приложением 1 к настоящему приказу.

2 Назначить ответственного:

2.1 за обработку и хранение персональных данных на бумажных носителях генерального директора Салпагарову О.Р.;

2.2 за автоматизированную обработку персональных данных, необходимую для исполнения требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физлиц и единого социального налога, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование. Заполнение первичной статистической документации в соответствии с Трудовым, Налоговым кодексом и т.д., и т.п. бухгалтера Гладских Н.В.*

3 Утвердить места хранения материальных носителей персональных данных в соответствии с приложением 2 к настоящему приказу.

4 Хранить материальные носители персональных данных только в утвержденных местах.

5 Утвердить инструкцию ответственных лиц, допущенных к обработке персональным данных в соответствии с приложением 3 к настоящему приказу.

6 Контроль за исполнением настоящего приказа оставляю за собой.

* В соответствии с договором на оказании услуг от 30.10.2015. Индивидуальный предприниматель Гладских Н.В, организует отправку отчетности в: Отделение Пенсионного Фонда по КЧР по г. Черкесску; в Межрайонную ИФНС № 3 по КЧР с персональными данными работников через программу Контур-экстерн (отчетность через интернет) с подписью представителя Гладских Надежды Викторовна по доверенности на передачу электронной отчетности с использованием средств криптографической защиты информации и электронной цифровой подписи.

Генеральный директор  О.Р. Салпагарова

Приложение 1 к приказу ООО
«КЛИНИКА «ВАШ ДОКТОР»
№1-4/2016 от 04.04.2016

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «КЛИНИКА «ВАШ ДОКТОР»

1 Общие положения

1.1 Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона Российской Федерации «О персональных данных» № 152-ФЗ от 27 июля 2006 г. а также иных нормативно-правовых актов Российской Федерации в области защиты и обработки персональных данных и действует в отношении всех персональных данных (далее – Данных), которые Организация (далее по тексту – Оператор) может получить от субъекта персональных данных, являющегося стороной по договору оказания медицинских услуг (пациент или его законный представитель), гражданско-правовому договору, а так же от субъекта персональных данных, состоящего с Оператором в отношениях, регулируемых трудовым законодательством (далее – Работника).

1.2 Оператор обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09. 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных документов уполномоченных органов.

1.3 Изменение Политики

1.4 Оператор имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.5 Действующая редакция хранится в месте нахождения Оператора по адресу: 369000, КЧР, г. Черкесск, ул. Ставропольская, 40А. Электронная версия Политики – на сайте организации по адресу: vachdoctor09.info.

2 Термины и принятые сокращения

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

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.

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Персональные данные, сделанные общедоступными субъектом персональных данных – ПД, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

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;

Оператор – организация, обрабатывающая персональные данные.

3 Обработка персональных данных

3.1 Получение ПД.

3.1.1 Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только у третьей стороны, то Субъект должен быть уведомлен об этом или от него должно быть получено согласие.

3.1.2 Оператор должен сообщить Субъекту о целях, предполагаемых источниках и способах получения ПД, характере подлежащих получению ПД, перечне действий с ПД, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа Субъекта дать письменное согласие на их получение.

3.1.3 Документы, содержащие ПД создаются путем:

- копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
- внесения сведений в учетные формы;
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

3.2 Обработка ПД

3.2.1 Обработка ПД осуществляется:

- с согласия Субъекта персональных данных на обработку его ПД в случаях, когда обработка ПД необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка ПД, доступ неограниченного круга лиц к которым предоставлен Субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными Субъектом персональных данных).

3.2.2 Цели обработки ПД:

- обеспечение организацией оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 г. № 323-ФЗ; «Об обязательном медицинском страховании граждан в Российской Федерации» от 29 ноября 2010 г. № 326-ФЗ; «Правила предоставления медицинскими организациями платных медицинских услуг» утвержденные Постановлением Правительства Российской Федерации от 04.10.2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

3.2.3 Категории Субъектов персональных данных.
Оператором обрабатываются ПД следующих Субъектов персональных данных:

- физические лица, состоящие с Оператором в трудовых отношениях;
- физические лица, прекратившие трудовые отношения с Оператором; физические лица, являющиеся кандидатами на работу у Оператора; физические лица, состоящие с Оператором в гражданско-правовых отношениях;
- физические лица, обратившиеся к Оператору за медицинской помощью.

3.2.4 ПД, обрабатываемые Оператором:

- данные полученные при осуществлении трудовых отношений;
- данные полученные для осуществления отбора кандидатов на работу;
- данные полученные при осуществлении гражданско-правовых отношений;
- данные полученные при оказании медицинской помощи.

3.2.5 Обработка ПД ведется:

- с использованием средств автоматизации;
- без использования средств автоматизации.

3.3 Хранение ПД

3.3.1 ПД Субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

3.3.2 ПД, зафиксированные на бумажных носителях хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

3.3.3 ПД Субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках.

3.3.4 Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

3.3.5 Хранение ПД в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.4 Уничтожение ПД

3.4.1 Уничтожение документов (носителей), содержащих ПД производится путем дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

3.4.2 ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

3.4.3 Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

3.5 Передача ПД

3.5.1 Оператор передает ПД третьим лицам в следующих случаях:

- Субъект выразил свое согласие на такие действия
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

3.5.2 Перечень лиц, которым передаются ПД.
Третьи лица, которым передаются ПД:

- Пенсионный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- Страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- Банки для перечисления заработной платы (на основании договора);
- Правоохранительные органы в случаях, установленных законодательством.

4 Защита ПД

4.1 В соответствии с требованиями нормативных документов Оператором создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

4.2 Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

4.3 Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами.

4.4 Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

4.5 Основными мерами защиты ПД, используемыми Оператором, являются:

4.5.1 Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением Оператором и его сотрудниками требований к защите ПД;

4.5.2 Определение актуальных угроз безопасности ПД при их обработке в ИСПД, и разработка мер и мероприятий по защите ПД;

4.5.3 Разработка политики в отношении обработки персональных данных;

4.5.4 Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПД в ИСПД;

4.5.5 Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

4.5.6 Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4.5.7 Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

4.5.8 Сертифицированное программное средство защиты информации от несанкционированного доступа;

4.5.9 Сертифицированные межсетевой экран и средство обнаружения вторжения;

4.5.10 Соблюдаются условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ;

4.5.11 Обнаружение фактов несанкционированного доступа к ПД и принятия мер;

4.5.12 Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4.5.13 Ознакомление сотрудников Оператора, непосредственно осуществляющих обработку ПД, с:

- положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите ПД;
- документами, определяющими политику Оператора в отношении обработки ПД;
- Локальными актами по вопросам обработки персональных данных;
- Осуществление внутреннего контроля и аудита.

5 Основные права субъекта ПД и обязанности оператора

5.1 Основные права субъекта ПД:

Субъект имеет право на доступ к его персональным данным и следующим сведениям

- подтверждение факта обработки ПД оператором.
- правовые основания и цели обработки ПД;
- цели и применяемые оператором способы обработки ПД;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПД или которым могут быть раскрыты ПД на основании договора с оператором или на основании федерального закона;
- сроки обработки ПД, в том числе сроки их хранения;

- порядок осуществления субъектом ПД прав, предусмотренных настоящим Федеральным законом;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка поручена или будет поручена такому лицу;
- обращения к оператору и направлению ему запросов;
- обжалование действий или бездействия оператора.

5.2 Обязанности Оператора.

Оператор обязан:

- при сборе ПД предоставить информацию об обработке ПД;
- в случаях, если ПД были получены не от субъекта ПД, уведомить субъекта;
- при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД а также от иных неправомерных действий в отношении ПД;
- давать ответы на запросы и обращения Субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.

Приложение 2 к приказу ООО
«КЛИНИКА «ВАШ ДОКТОР»
№1-4/2016 от 04.04.2016

Перечень мест хранения материальных носителей персональных данных и ответственных лиц

N п/п	Категория персональных данных	Место хранения	Ответственное лицо (должность, ФИО)
1.	Бумажные носители Пдн, в т.ч, личные дела; материалы по учету рабочего времени; личная карточка Т-2;	Железный сейф (Черкесск, ул. Ставропольская, 40А, каб.5).	Врач рентгенолог – Салпагарова О.Р.
2.	Электронные носители персональных данных*	Компьютер в офисе бухгалтера с защищенным входом (пароль) с программой антивирус «Kaspersky» (г. Черкесск, пл. Кирова 1 оф. 3).	Бухгалтер – Гладских Н.В.

* В соответствии с договором на оказании услуг от 30.10.2015. Индивидуальный предприниматель Гладских Н.В, организует отправку отчетности в: Отделение Пенсионного Фонда по КЧР по г. Черкесску; в Межрайонную ИФНС № 3 по КЧР с персональными данными работников через программу Контур-экстерн (отчетность через интернет) с подписью представителя Гладских Надежды Викторовна по доверенности на передачу электронной отчетности с использованием средств криптографической защиты информации и электронной цифровой подписи.

Приложение 3 к приказу ООО
«КЛИНИКА «ВАШ ДОКТОР»
№1-4/2016 от 04.04.2016

ИНСТРУКЦИЯ
ответственных лиц, допущенных к обработке персональных данных

1 Общие положения

1.1 Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- «Требований к защите персональных данных при их обработке в информационных системах персональных данных» утвержденной постановлением Правительства Российской Федерации от 01.11.2012 №1119.

1.2 Данная инструкция определяет общие обязанности, права и ответственность пользователя информационных систем по обеспечению информационной безопасности при работе со сведениями конфиденциального характера.

1.3 Пользователем ИС (далее – Пользователь) является работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС.

1.4 Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5 Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2 Обязанности пользователя

2.1 При выполнении работ в ИС Пользователь обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, правила работы и порядок регистрации в ИС, доступа к информационным ресурсам ИС;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее - АРМ);
- хранить втайне свои идентификационные данные (имена, пароли и т. д.);
- выполнять требования, предъявляемые к парольной системе (нормативы на длину, состав, периодичность смены пароля и т. д.), осуществлять вход на АРМ только под своими идентификационными данными;
- передавать для хранения установленным порядком свое индивидуальное устройство идентификации, личную ключевую дискету и другие реквизиты разграничения доступа, только руководителю своего подразделения или администратору безопасности ИС (ответственному за информационную безопасность подразделения);
- выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей ИС;
- немедленно вызывать администратора безопасности ИС и ставить в известность руководителя подразделения в случае утери персональной ключевой дискеты, индивидуального устройства идентификации или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного

доступа (НСД) к защищенной АРМ, несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ, ставить в известность администратора безопасности ИС при необходимости внесения изменения в состав аппаратных и программных средств АРМ;
- работать в ИС только в разрешенный период времени;
- немедленно выполнять предписания администраторов безопасности ИС, предоставлять свое АРМ администратору безопасности для контроля;
- ставить в известность администраторов ИС в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т. п.), а также перебоев в системе электроснабжения;
- осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;
- уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;
- сообщать руководителю своего подразделения обо всех проблемах, связанных с эксплуатацией ИС.

2.2 Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;
- самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИС (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формуляром АРМ;
- осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации, в том числе для временного хранения;
- оставлять включенное без присмотра АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);
- передавать кому-либо свое индивидуальное устройство идентификации (персональную ключевую дискету) в нарушение установленного порядка, делать неучтенные копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИС (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора безопасности ИС (ответственного за безопасность информации) и руководителя своего подразделения;
- подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;

- осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;
- фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;
- разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;
- вносить изменения в файлы, принадлежащие другим пользователям.

3 Права пользователя

3.1 Пользователь имеет право:

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;
- своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;
- требовать от администратора безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4 Правила работы в сетях общего доступа

4.1 Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИС, должна производиться при служебной необходимости.

4.2 При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусной защиты, средств от несанкционированного доступа и т. д.);
- передавать по Сети защищаемую информацию без использования средств защиты каналов связи;
- запрещается загружать из Сети программное обеспечение;
- запрещается посещение сайтов сомнительной репутации (аморального содержания, содержащие нелегально распространяемое программное обеспечение или иной контент);
- запрещается нецелевое использование подключения к сети.

5 Ответственность пользователя

5.1 Пользователь несет персональную ответственность за:

- ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, индивидуального средства идентификации и целостность установленного программного обеспечения.
- разглашение сведений, отнесенных к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы.

5.2 Ответственность за нарушение функционирования ИС, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

5.3 Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами.