Приложение № 1 к Приказу № 29 от 15 декабря 2022 года

ПОЛОЖЕНИЕ

о системе видеонаблюдения в Обществе с ограниченной ответственностью «Центр стоматологии доктора Музыки» (ООО «Центр стоматологии доктора Музыки»)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано в соответствии с Федеральным законом РФ "О персональных данных" от 27.07.2006 N 152-ФЗ, Постановлением Правительства РФ от 17.11.2007 N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", Федеральным законом от 06.03.2006 г. №35 «О противодействии терроризму», Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах здоровья граждан РФ».
1.2. Под видеонаблюдением понимается непосредственное осуществление видеонаблюдения посредством использования видеокамер для получения видеоинформации об объектах и помещениях, а также запись полученного изображения и его хранение для последующего использования.
1.3. Система видеонаблюдения является открытой, ведется с целью обеспечения безопасности работников организации и не может быть направлена на сбор информации о конкретном человеке.
1.4. Система открытого видеонаблюдения в Обществе с ограниченной ответственностью «Центр стоматологии доктора Музыки» (далее по тексту - Организация) является элементом общей системы безопасности Организации, направленной на обеспечение безопасной организации оказания медицинских услуг, поддержание дисциплины и порядка в Организации, предупреждение возникновения чрезвычайных ситуаций и обеспечение сохранности имущества.
1.5. Настоящее Положение обязательно для работников, пациентов и (или) посетителей ООО «Центр стоматологии доктора Музыки». Настоящее Положение подлежит размещению на официальном сайте Организации и находится в свободном доступе для работников и посетителей «Центр стоматологии доктора Музыки».
1.6. С целью противодействия терроризму и совершению противоправных действий, «Центр стоматологии доктора Музыки» обязано вести наблюдение за состоянием обстановки на всей территории, архивировать и хранить данные в течение 30 дней (постановление Правительства от 13.01.2019 г. № 8). Система видеонаблюдения в медицинской организации необходима для защиты посетителей и персонала от угроз терроризма и противоправных действий, несанкционированного вторжения (ч.13 ст. 30 Федерального закона от 30.12.2009г. № 384 «Технический регламент о безопасности зданий и сооружений»), а также контроля качества оказываемых в организации медицинских услуг.

2. ПОРЯДОК ОРГАНИЗАЦИИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

2.1. Решение об установке системы видеонаблюдения принимается руководителем Организации, видеоконтроль вводится соответствующим приказом.
2.2. Лица, являющиеся сотрудниками организации на момент введения системы видеоконтроля, должны в письменной форме выразить свое согласие или несогласие на введение данной системы (заполнение согласия на обработку персональных данных). Если работник не согласен на изменение условий трудового договора, то после выполнения процедур, предусмотренных Трудовым кодексом РФ (письменное уведомление о предстоящих изменениях, предложение другой работы) трудовой договор с ним может быть расторгнут по пункту 7 статьи 77 ТК РФ.
2.3. Сотрудники, вновь принимаемые на работу, выражают свое согласие на проведение видеоконтроля путем заполнения формы согласия на обработку персональных данных.
2.4. Посетители организации информируются о системе видеоконтроля путем размещения специальных информационных табличек в зонах видимости видеокамер.
2.5. Система видеонаблюдения предприятия входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства.
2.6. Места установки видеокамер в Организации определяются по мере необходимости в соответствии с конкретными задачами.
2.7. Видеокамеры устанавливаются в местах, открытых для общего доступа (территория, входы в здание, коридоры), а также в помещениях, где оказываются медицинские услуги (процедурный кабинет, кабинеты врачей и т.п).
2.8. Установка видеокамер не допускается в туалетных комнатах, комнатах для переодевания работников и в иных местах, связанных с осуществлением личных нужд работников, посетителей.

2.9. Запрещается использование устройств, предназначенных для негласного получения информации (скрытых камер).

3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

3.1. Целью системы видеонаблюдения является создание условий для антитеррористической защищенности в Организации, безопасности персонала и пациентов, сохранности имущества, своевременного реагирования при возникновении чрезвычайных ситуаций, осуществление внутреннего контроля качества и безопасности медицинской деятельности. 3.2. Задачами организации видеонаблюдения являются:
− контроль за обстановкой в помещениях и на территории Организации, обеспечение защиты от несанкционированного проникновения на территорию и в здание посторонних лиц и транспортных средств;
− своевременное реагирование при возникновении опасных и чрезвычайных ситуаций, в т.ч. вызванных террористическими актами на территории Организации;
− охрана жизни, предупреждение и минимизация рисков травматизма работников Организации и посетителей;
− установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы работником);
− обеспечение противопожарной защиты зданий и сооружений;

− повышение ответственности всех сотрудников за качество своей профессиональной деятельности и выполнение должностных обязанностей;
− раннее выявление причин и признаков опасных ситуаций, их предотвращение и устранение;
− пресечение противоправных действий со стороны работников Организации и посетителей; − охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а также предупреждение случаев хищения имущества организации и/или работников/посетителей;
− отслеживание, фиксация, своевременная передача изображений и данных об объектах видеонаблюдения;
− информационное обеспечение принятия решений заведующим Учреждением;
− предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.
3.3. Система видеонаблюдения должна обеспечивать:
− видео фиксацию текущего состояния объекта видеонаблюдения;
− сохранение архива видеозаписей для последующего анализа;
− воспроизведение ранее записанной информации;
− оперативный доступ к архиву видеозаписей за конкретный период времени и с определённых видеокамер.
3.4. Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред имуществу. В случае необходимости материалы видеозаписей, полученных камерами видеонаблюдения, будут использованы в качестве доказательства в уголовном или гражданском судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего соответствующее противоправное действие.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность сотрудников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой персональных данных.
4.2. Организация обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", и принятыми в соответствии с ним нормативными правовыми актами.
4.3. Обработка персональных данных должна осуществляться на законной основе и ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных.
4.4. Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

5. ПРОСМОТР, ХРАНЕНИЕ ДАННЫХ ВИДЕОНАБЛЮДЕНИЯ И ПЕРЕДАЧА ДАННЫХ ТРЕТЬИМ ЛИЦАМ

5.1. Запись камер видеонаблюдения осуществляется постоянно (24 часа в сутки) и подлежит хранению в течение 30 дней.
5.2. Система видеонаблюдения предполагает запись информации на жесткий диск видеорегистратора / в облачное хранение ПАО «Ростелеком», которая не подлежит перезаписи и длительному хранению, уничтожается автоматически через 30 дней.
5.3. Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи, редактированию, передачи третьим лицам.
5.4. Отображение процесса видеозаписи в режиме реального времени производится на экраны, установленные:
− в кабинетах Директора, руководителя обособленного подразделения с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций.
5.5. Доступ к просмотру записей видеонаблюдения, хранящимся установленный период на жестком диске видеорегистратора, облачного хранилища имеет Директор Организации, заместитель директора, руководитель обособленного подразделения. На основании письменного разрешения директора Организации другие работники Организации могут быть допущены к просмотру записей видеонаблюдения, при условии принятия ими на себя обязательств о неразглашении персональных данных третьих лиц.
5.6. Обеспечением конфиденциальности является пароль доступа к информации видеорегистратора/облачного хранилища, который известен лицам, имеющим право на просмотр.
5.7. Просмотр записанных изображений может осуществляться исключительно при личном участии директора Организации в условиях ограниченного доступа (при отсутствии посторонних лиц).
5.8. Для защиты публичных интересов (т.е. выявление факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи, сотрудники полиции.
5.9. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по письменному запросу следственных и судебных органов, а также по письменному запросу работников, изображенных на видеозаписи). Вопрос о передаче записей решает Директор Организации.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении требований Федерального закона "О персональных данных", несут предусмотренную законодательством Российской Федерации ответственность.
6.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных подлежат возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от

возмещения имущественного вреда и понесенных субъектом персональных данных убытков.
6.3. Работникам Организации запрещается: препятствовать работе системы видеонаблюдения путем регулировки направления (обзора) камер видеонаблюдения, загораживать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения, отключать электропитание камер системы видеонаблюдения. За причинение материального вреда и порчу камер системы видеонаблюдения работники Организации несут ответственность в соответствии с действующим законодательством Российской Федерации.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящее положение, изменения, дополнения к нему, утверждаются приказом директора учреждения.
7.2. Ознакомление работников учреждения с настоящим положением, изменениями и дополнениями к нему, проводится в обязательном порядке под роспись