

ПОЛОЖЕНИЕ

о системе видеонаблюдения в ГАУЗ «МКДЦ»

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», статьей 21 Трудового Кодекса РФ.

1.2. Под видеонаблюдением в Государственном автономном учреждении здравоохранения «Межрегиональный клинико-диагностический центр» (далее - Организация) понимается непосредственное осуществление видеонаблюдения посредством использования видеокамер для получения видеoinформации 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. Настоящее Положение обязательно для работников, пациентов и (или) посетителей Организации, находится в свободном доступе, размещен на официальном сайте.

1.5. Система видеонаблюдения в 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 генеральным директором Организации.

2.2. Система видеонаблюдения Организации входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства.

2.3. Места установки видеокамер на территории Организации определяются по мере необходимости в соответствии с конкретными задачами.

2.4. Видеокамеры устанавливаются в местах, открытых для общего доступа (территория, входы в здание, коридоры), а также в помещениях, где оказываются медицинские услуги.

2.5. Установка видеокамер не допускается в туалетных комнатах, комнатах для переодевания работников и в иных местах, связанных с осуществлением личных нужд работников, посетителей.

2.6. Работники, пациенты и посетители Организации информируются о системе видеоконтроля путем размещения специальных информационных табличек в зонах видимости видеокамер.

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

3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

3.1. Целью системы видеонаблюдения является:

3.1.1. создание условий для антитеррористической защищенности в Организации,

3.1.2. безопасность работников, пациентов и посетителей,

3.1.3. сохранность имущества,

3.1.4. своевременное реагирование при возникновении чрезвычайных ситуаций,

3.1.5. осуществление внутреннего контроля качества и безопасности медицинской деятельности,

3.2. Задачами организации видеонаблюдения являются:

3.2.1. контроль за обстановкой в помещениях и на территории Организации,

3.2.2. обеспечение защиты от несанкционированного проникновения на территорию и в здание посторонних лиц и транспортных средств;

3.2.3. своевременное реагирование при возникновении опасных и чрезвычайных ситуаций, в т.ч. вызванных террористическими актами на территории Организации;

3.2.4. обеспечение противопожарной защиты зданий и сооружений;

3.2.5. пресечение противоправных действий со стороны работников Организации, пациентов и посетителей;

3.2.6. предупреждение случаев хищения имущества Организации и/или работников, пациентов и посетителей;

3.3. 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 работников 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, которая не подлежит перезаписи и длительному хранению, уничтожается автоматически по мере заполнения памяти жесткого диска через 30 дней.

5.3. Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи с жесткого диска видеорегистратора, редактированию, передачи третьим лицам.

5.4. Доступ к просмотру записей видеонаблюдения, хранящимся установленный период на жестком диске видеорегистратора, имеет: генеральный директор, заместители генерального директора, начальник управления безопасности, начальник юридической службы, а также иные лица, уполномоченные генеральным директором.

5.5. Просмотр записей с камер видеонаблюдения должен осуществляться исключительно в зоне ограниченного доступа лицами, имеющими право доступа к видеоматериалам.

5.6. Передача записей камер видеонаблюдения третьей стороне допускается только в случаях, предусмотренных действующим законодательством, по согласованию с генеральным директором.

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.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящее положение, изменения, дополнения к нему, утверждаются приказом генерального директора Организации.

7.2. Ознакомление работников Организации с настоящим положением, изменениями и дополнениями к нему, проводится в обязательном порядке под роспись.