Положение о видеонаблюдении в ООО «Дантист»

1. Общие положения

1.1. Положение о видеонаблюдении в ООО «Дантист» (далее – Положение, Организация) определяет порядок использования видеоаппаратуры и организации системы видеонаблюдения посредством использования видеокамер для получения видеоинформации об объектах, записи полученного изображения и хранения его для дальнейшего использования в служебных помещениях Организации.

1.2. Система видеонаблюдения является элементом общей системы безопасности Организации, направленной на контроль за качеством и безопасностью медицинской деятельности, обеспечение личной безопасности работников, пациентов и посетителей Организации, сохранности их имущества, усиление контроля за использованием рабочего времени, укрепление трудовой дисциплины работников, предупреждение возникновения чрезвычайных ситуаций и обеспечение объективности расследования несчастных случаев, трудовых и иных конфликтов в случае их возникновения.

1.3. Видеонаблюдение в Организации ведется круглосуточно при помощи видеокамер открытого видеонаблюдения. Запрещается использование устройств, предназначенных для негласного получения информации (скрытых камер). Не допускается установка видеокамер в туалетных комнатах, комнатах отдыха.

1.4. Процесс оказания медицинской помощи относится к врачебной тайне, видеозапись относится к персональным данным, поэтому необходимо обеспечить конфиденциальность персональных данных лиц, которые участвуют в осуществлении медицинской деятельности, лиц, которым оказывается медицинская помощь, а также лиц, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования.

1.5. Положение обязательно для работников Организации. Каждый работник подлежит ознакомлению с ним под личную подпись. Выписки из Положения подлежат размещению на видных местах.

1.6. Локальные нормативные акты Работодателя и условия трудовых договоров с работниками, регламентирующие видеонаблюдение, в обязательном порядке согласовываются с руководителями отдела кадров и Службы безопасности Организации.

2. Порядок организации системы видеонаблюдения

2.1. Система видеонаблюдения устанавливается в Организации на основании Положения.

2.2. Система видеонаблюдения Организации входит в систему контроля доступа и включает в себя ряд устройств: видеокамеры, мониторы, записывающие устройства, системные блоки и иное техническое оборудование, составляющие инфраструктуру указанной системы.

2.3. Установка системы видеонаблюдения осуществляется в соответствии с ее целями и задачами согласно проектно-технической документации и при условии периодических контрольных проверок ее технического состояния с ведением специального журнала об этом.

2.4. Пациенты и посетители информируются посредством размещения специальных информационных табличек с надписями и символами, а также размещением информации о ведущемся видеонаблюдении на официальном сайте Организации.

2.5. Функции по обеспечению безопасности хранения, настройке и изменению параметров системы, конфигурирование системы, управление параметрами архивирования, учетными

записями доступа к системе видеонаблюдения (логины и пароли) и назначение прав доступа осуществляет руководитель Службы безопасности (в его отсутствие – лицо, его замещающее).

2.6. Обеспечением конфиденциальности является пароль доступа к информации видеорегистратора, хранящийся у руководителя Службы безопасности (лица, его замещающего).

2.7. Информация, собранная при помощи систем видеонаблюдения, относится к биометрическим персональным данным, за разглашение которых виновные лица могут быть привлечены к ответственности.

3. Цели и задачи системы видеонаблюдения

3.1. Система видеонаблюдения призвана выполнять ряд практических задач:

3.1.1. Обеспечение качества и безопасности медицинской деятельности.

3.1.2. Повышение эффективности действий всех подразделений Организации при возникновении проблемных ситуаций.

3.1.3. Обеспечение противопожарной защиты объектов и служебных помещений Организации.

3.1.4. Обеспечение антитеррористической защиты и безопасности работников и посетителей Организации на территории Организации, охраны правопорядка, защиты имущества Организации, работников, посетителей от противоправных посягательств.

3.1.5. Совершенствование системы информирования и оповещения работников и посетителей Организации об угрозе возникновения кризисных ситуаций.

3.1.6. Пресечение противоправных действий со стороны работников и посетителей Организации.

3.2. Видеонаблюдение осуществляется с целью документальной фиксации возможных противоправных действий, которые могут нанести вред работникам, пациентам и посетителям Организации, их имуществу. Материалы видеозаписей могут быть использованы в уголовном, административном и гражданском судопроизводствах, предварительном расследовании для доказывания фактов совершения противоправных деяний, а также для установления личностей правонарушителей. Указанные материалы могут быть переданы по требованию суда или сотрудников правоохранительных или иных уполномоченных органов в соответствии с законодательством РФ.

4. Порядок доступа, сроки хранения, уничтожения и передача третьим лицам записей системы видеонаблюдения

4.1. Доступ к месту хранения записей систем видеонаблюдения имеет руководитель Службы безопасности (в его отсутствие – лицо, его замещающее).

4.2. Ответственным за организацию хранения и уничтожения записей систем видеонаблюдения является руководитель Службы безопасности (в его отсутствие – лицо, его замещающее).

4.3. Ответственным за организацию хранения и уничтожения записей систем видеонаблюдения процесса оказания медицинской помощи назначается специалист с медицинским образованием.

4.4. Система видеонаблюдения производит цикличную запись информации на жесткий диск видеорегистратора и уничтожается (перезаписывается) автоматически по мере заполнения жесткого диска.

4.5. Срок хранения видеозаписей составляет не менее 48 (сорока восьми) часов. Если камеры видеонаблюдения зафиксировали нестандартную ситуацию, то для таких записей устанавливается специальный срок хранения – 1(один) месяц. В случае необходимости срок может быть увеличен приказом главного врача Организации.

4.6. Носители с записями камер системы видеонаблюдения, на которых зафиксирована нестандартная ситуация, подлежат хранению в опечатанном виде в сейфе, расположенном в кабинете руководителя Службы безопасности.

4.7. Записи систем видеонаблюдения не могут выкладываться в интернет, локальную сеть или доводиться до всеобщего сведения без письменного согласия лиц, в отношении которых эти записи были созданы.

4.8. Лицо, виновное в причинах нарушения конфиденциальности записей систем видеонаблюдения, несет ответственность в порядке, предусмотренном действующим законодательством Российской Федерации.

4.9. Использование записей систем видеонаблюдения в личных целях запрещено.

4.10. По истечении срока хранения записей систем видеонаблюдения они подлежат уничтожению.

4.11. Запись информации видеонаблюдения является информацией ограниченного распространения, не подлежит передаче третьим лицам, за исключением случаев, предусмотренных действующим законодательством Российской Федерации (в т. ч. по письменному запросу следственных и судебных органов).

4.12. Решение о выдаче (выемке) записей систем видеонаблюдения по запросам принимает руководитель медицинской организации.

5. Меры по обеспечению защиты персональных данных

5.1. Видеонаблюдение в медицинской организации является обращением с биометрическими персональными данными.

5.2. Организация обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей оператора по обработке персональных данных, а также получить согласие работников и пациентов на обработку их персональных данных, включая биометрические персональные данные.

5.3. Обработка персональных данных осуществляется на основании Положения о защите персональных данных. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных.

5.4. 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.

5.5. По всем фактам возможного нарушения своих прав и законных интересов работники, пациенты и посетители могут обращаться к руководителю Службы безопасности Организации.

6. Ответственность за нарушения правил обработки персональных данных

6.1. Лица, виновные в нарушении требований Положения, несут предусмотренную законодательством РФ ответственность.

6.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством РФ.

6.3. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.