Утверждаю
Главный врач Клиники,
Генеральный директор ООО «Ля Дентик»
_____
Светлова Л.А.
(приказ №23 от 1.09.2023

ПОЛОЖЕНИЕ

о системе видеонаблюдения в Клинике ООО «Ля Дентик»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В соответствии с требованиями Федерального закона от 06.03.2006 г. №35 «О противодействии терроризму», Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», Федерального закона от 21.11.2011 г. №323-ФЗ «Об основах здоровья граждан РФ», Федерального закона от 02.07.2021 г. №311-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации», Постановления Правительства РФ от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и Постановления Правительства РФ от 13 января 2017 г. № 8 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)».

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. С целью противодействия терроризму и совершению противоправных действий, Клиника обязана вести видеонаблюдение за состоянием обстановки в режиме реального времени на всех территориях, помещениях и в отдельных кабинетах, архивировать и хранить данные в течение 30 суток. Система видеонаблюдения (далее – СВН) в Клинике необходима для защиты (безопасности) персонала, пациентов и посетителей от угроз терроризма и противоправных действий, несанкционированного вторжения (ч.13 ст. 30 Федерального закона от 30.12.2009 г. №384 «Технический регламент о безопасности зданий и сооружений»), а также внутреннего контроля качества и безопасности медицинской помощи.

1.4. СВН является открытой и не может быть направлена на сбор информации о конкретном человеке, направлена на контроль дисциплины сотрудников и порядка в Клиники, предупреждения возникновения чрезвычайных ситуаций и обеспечения сохранности имущества. 1.5. Настоящее Положение обязательно для работников, пациентов и (или) посетителей Клиники. Настоящее Положение подлежит размещению на официальном сайте и находится в свободном доступе для работников, пациентов и посетителей Клиники.

2. ПОРЯДОК ОРГАНИЗАЦИИ СВН

2.1. Решение об установке СВН принимается главным врачом Клиники, видеоконтроль вводится соответствующим приказом.

2.2. Сотрудники, вновь принимаемые на работу, выражают свое согласие на проведение видеоконтроля путем заполнения формы согласия на обработку персональных данных.

2.3. Лица, являющиеся сотрудниками Клиники на момент введения СВН, 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 трудовой договор с ним может быть расторгнут по пункту 7 статьи 77 ТК РФ.

2.4. Посетители организации информируются о СВН путем размещения специальных информационных табличек в зонах видимости видеокамер, а также на информационном стенде, на сайте Клиники.

2.5. СВН Клиники входит в систему контроля доступа и включает в себя ряд устройств: камеры, мониторы, записывающие устройства (видеорегистраторы).

2.6. Места установки видеокамер в Клинике определяются по мере необходимости в соответствии с конкретными задачами решением главного врача.

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, душевых комнатах для пациентов и работников Клиники и в комнатах для переодевания работников.

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

2.10. СВН должна иметь резервный АРМ для дублирования и хранения записываемой информации.

2.11. Лица, ответственные за эксплуатацию, работоспособность и защиту информации в СВН назначаются приказом главного врача.

3. ЦЕЛИ И ЗАДАЧИ СВН

3.1. Целью СВН является создание условий для антитеррористической защищенности в Клинике, 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 на территориях и в помещениях Клиники, обеспечение защиты от несанкционированного проникновения на территории, в здания и в помещения посторонних лиц и транспортных средств;

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

– охрана жизни, предупреждение и минимизация рисков травматизма работников Клиники и посетителей;

– установление достоверности фактов при расследовании несчастных случаев (запись события, регистрация времени, места и участников, причин получения травмы работником, пациентом, посетителем);

– 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, пациентов и 5 посетителей Клиники;

– охрана имущества, предупреждение и устранение причин (последствий) деятельности, приводящей к порче имущества, а также предупреждение случаев хищения имущества Клиники и/или работников/посетителей;

– отслеживание, фиксация, своевременная передача изображений и данных об объектах видеонаблюдения;

– информационное обеспечение принятия решений главным врачом;

– предоставление информации по запросам соответствующих служб и государственных органов в случаях, предусмотренных действующим законодательством.

3.3. СВН 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, могут быть использованы в качестве доказательства в уголовном, гражданском или административном судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего соответствующее противоправное действие.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ (СЛУЖЕБНОЙ ИНФОРМАЦИИ)

4.1. СВН позволяет отслеживать деятельность сотрудников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой служебной информации.

4.2. Клиника обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, в части касающейся предусмотренных Федеральным законом №152-ФЗ от 27.07.2007 года «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами.

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

5.1. СВН предполагает запись информации в режиме реального времени на жесткий диск видеорегистратора и резервного автоматизированного рабочего места (далее – АРМ), которая не подлежит перезаписи и длительному хранению:

– для видеокамер, установленных для обеспечения антитеррористической защищенности Клиники, уничтожается автоматически по мере заполнения памяти жесткого диска не менее, чем через 30 суток;

– для видеокамер, установленных для осуществления внутреннего, контроля качества и безопасности оказания медицинских услуг, уничтожается автоматически по мере заполнения памяти жесткого диска до 14 суток.

5.2. Запись информации видеонаблюдения является конфиденциальной, не подлежит перезаписи с жестких дисков видеорегистраторов и резервного АРМ, редактированию. Исключение составляют случаи официального письменного обращения с разрешения главного врача Клиники.

5.3. Отображение процесса видеозаписи в режиме реального времени производится на экраны, установленные:

– в кабинете главного врача с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;

– на ресепшн, с целью своевременного реагирования на возникновение признаков и причин опасных ситуаций;

5.4. Разрешение доступа к просмотру записей видеонаблюдения, хранящихся установленный период на жестком диске видеорегистратора и резервного АРМ, осуществляется:

– для просмотров записей в общих помещениях Клиники - с разрешения главного врача Клиники;

– для просмотров записей в кабинетах Клиники - с разрешения главного врача Клиники;

– для просмотров записей, установленных для антитеррористической защищенности Клиники - с разрешения главного врача.

На основании письменного разрешения главного врача Клиники, другие работники Клиники могут быть допущены к просмотру записей видеонаблюдения, при условии принятия ими на себя обязательств о неразглашении персональных данных третьих лиц только в присутствии ответственного за организацию работы СВН или лица, его замещающего.

5.5. Обеспечением конфиденциальности является пароль доступа к информации видеорегистратора. Генерация и выдача паролей доступа осуществляется ответственным за организацию работы СВН, назначенным приказом главного врача Клиники посредством ведения «Журнала генерации, учета и выдачи паролей доступа» под личную роспись. Смена пароля или его продление осуществляется не реже одного раза в год (либо при увольнении этих должностных лиц).

5.6. Просмотр записанных изображений может осуществляться исключительно при личном участии Главного врача Клиники.

5.7. Для защиты публичных интересов (т.е. выявление факта совершения правонарушения) в просмотре могут участвовать лица, изображенные на записи и сотрудники полиции (и других правоохранительные органы РФ).

5.8. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях (по письменному мотивированному запросу следственных и судебных органов, а также по письменному мотивированному запросу работников, изображенных на видеозаписи). Решение о передаче записей принимает главный врач Клиники.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении требований Федерального закона №152-ФЗ от 27.07.2007 года «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

6.2. Моральный и материальный 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 Клиники (кроме уполномоченных на то лиц) ЗАПРЕЩАЕТСЯ: препятствовать работе СВН путем регулировки направления (обзора) камер видеонаблюдения, загораживать, закрывать камеры или каким-либо иным способом препятствовать производству видеонаблюдения, отключать электропитание камер СВН. За причинение материального вреда и порчу камер СВН работники Клиники несут ответственность в соответствии с действующим законодательством Российской Федерации.

7. ОРГАНИЗАЦИЯ ВСЕСТОРОННЕГО ОБЕСПЕЧЕНИЯ РАБОТЫ СВН

7.1. Ответственность за проведение технического обслуживания, в том числе проведения ремонтных работ для поддержания работоспособности СВН возлагается на Светлову Л.А.

7.2. Ответственность за работоспособность программно-аппаратного комплекса СВН, в том числе его модернизацию (обновление операционных систем, САВЗ, системы разграничения доступа и т.д.) возлагается на Светлову Л.А.

7.3. Выполнение работ, указанных в п.п. 7.1. и 7.2., в том числе в нерабочее время (выходные, нерабочие и праздничные дни) проводить только по согласованию с ответственным за организацию работы СВН с записью в журнале учета вскрытия помещений (приложение 2).

7.4. Ответственность за предотвращение неправомерного доступа к защищаемой информации, хранящейся на магнитных накопителях, контроль за ее использованием, возлагается на Светлову Л.А.

7.5. Организация информационной безопасности при эксплуатации СВН должна обеспечивать установленные сроки хранения, конфиденциальность и целостность информации и обеспечивается проведением следующих мероприятий:

– ограничением круга лиц, допущенных к информации с СВН, в соответствии с приказом главного врача;

– ограничением физического доступа к магнитным накопителям СВН путем опечатывания устройств, исключающих их вскрытие без нарушения оттиска печати ответственного за организацию работы СВН по ЗИ;

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение, изменения и дополнения к нему, утверждаются приказом главного врача Клиники.

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