Guidelines for the Use of Closed Circuit Television (CCTV) In GHS Facilities
Clinical Services Development Department
Institutional Care Division
Ghana Health Service

Updated in May 2011

Table of Contents

3.0 Keywords, Definitions, Abbreviations and Acronyms

Abbreviations and Acronyms

GHS: Ghana Health Service

CCTV: Closed Circuit Television

OEM: Original Equipment Manufacturer

FOV: Field Of View

3.1 Definitions

3.1.1 Parking lot: A designated parking area of a health facility where health workers park their official and personal vehicles.

3.1.2 Health facility: Any facility belonging to GHS examples, hospitals and directorates.

3.1.3 Recognizable image: Image not less than 50 percent of target to screen height ratio when viewed on a monitor without zoom.

3.1.4 Risk assessment: A formal, methodical process that evaluates risks to a transit system. The security portion of the risk assessment identifies security threats (both theft and crime) to the GHS facility; evaluates system vulnerabilities to those threats; and determines the consequences to people, equipment and property.

3.1.5 Hospital: A type of health facility designated for the purpose of providing healthcare to patients and clients. Hospital features and amenities may include information/waiting areas, equipment, restrooms, and other related amenities.

1. Introduction

Closed Circuit Television Cameras (CCTV) have become important crime prevention and security measure in modern life. They are situational measures that enable a locale to be kept under surveillance remotely. In many parts of the world CCTV coverage is found in both public and private buildings such as hospitals, buses, homes and on the streets. Hospitals house very expensive equipment and consumables such as drugs and supplies that are to be kept safe from theft. The use of Closed Circuit Television systems and the recording of security images is therefore an accepted practice for health institutions such as hospitals and clinics across the world. The reasons for the use of CCTV are many and varied but the main aim is to deter crime. This practice facilitates the apprehension and conviction of individuals involved in criminal activity. The five main assumptions underlying CCTV coverage usage to reduce crime are:

- ***To serve as a deterrence:*** That is, the potential offender becomes aware of the presence of CCTV; assesses the risks of offending in that location, and if the cost outweighs the benefits then the potential offender may choose either not to offend/cause the crime or to offend/cause the crime elsewhere.

- ***Fear of Detection:*** CCTV cameras capture images of offences taking place. In some cases this may lead to punishment and the removal of the offenders' ability to offend (either due to incarceration, or increased monitoring and supervision).

- ***To Induce Self discipline:*** CCTV could help induce self discipline by both a potential victim and potential offender. The CCTV camera may produce self-discipline through fear of surveillance, whether real or imagined.
    - **By potential victims**. They are reminded of the 'risk' of crime, therefore altering their behaviour accordingly.
    - **By potential offenders.** The threat of potential surveillance (whether the cameras are actually being monitored may be irrelevant) acts to produce a self discipline in which individuals police their own behaviour. Since the potential offender could never be sure whether they were being watched, they may police their own behaviours.

- ***Presence of a capable guardian:*** The 'Routine Activity Theory' suggests that for a crime to be committed there must be a motivated offender, a suitable target and the absence of a capable guardian. Any act that prevents the convergence of these elements will reduce the likelihood of a crime taking place. CCTV, as a capable guardian, may help to reduce crime.

- ***For Efficient deployment:*** CCTV cameras allow those monitoring the scene to determine whether police assistance is required. This ensures that police resources are called upon only when necessary.

Ghana health facilities however, continue to rely on "no-technological" options such as gates with security men, locks, good lighting and barriers such as walls and fence, which have proven not to be effective to safe guard their properties. Meanwhile, reports from hospitals and institutions indicate that, health facilities are still grapple with cases of theft of health facility properties such as handy high-value equipment, computer and their accessories, vehicle parts, drugs and other supplies.

The cost of these lost properties to health facilities can be quite substantial. Recently, infant abduction, violence against patients and staff are also gradually becoming a problem in our health facilities. It would therefore be of interests for management to begin to use security measures proven to be effective and efficient. CCTV is one such method that could help improve hospital security. For example, CCTV asset protection systems can enhance hospital security by safe guarding the facility's property. By viewing CCTV monitors health authorities, police and others may be able to more effectively pinpoint trouble spots, trouble times, activities etc., and anticipate/remove crime catalysts.

Staff and clients attitude are another areas of concern. As a by-product, CCTV can help both patients and staff to police their own behaviours to the extent that CCTV induces self-discipline in them. The few hospitals in the country that use CCTV attest to this assertion. The hospitals reported improvement in staff attitudes towards patients and their work. Thus, CCTV coverage in our health facilities could compliment efforts to improve customer care.

The variety of people who make up the typical hospital environment: (that is, staff (clinicians and non clinicians), patients, their relatives and friends, visitors, partners and sellers; coupled with the many entrances, different rooms and spaces and ease-of-movement around the building and premises makes use of technologically sound hospital security measures such as the use of CCTV imperative. This tool has proven to enhance security in health facilities across the world.

1.1 Purpose

This document is to provide recommendations and guidelines for the use of Closed Circuit Television (CCTV) security systems in hospitals and clinics.

The purpose is to ensure that hospitals and clinics achieve high levels of safety and security for the vital equipment and supplies, patients/clients and employees (health workers).

1.2 Vision

GHS envision that with the implementation of this improved surveillance system; health facilities properties will be intact.

1.3 Mission

GHS is committed to providing improved surveillance system through the provision of CCTV; manned at the facility management.

2. Policy Statement

The Ghana Health Service shall ensure that CCTV services are available at these levels - National, Regional, District, Sub-district/Facility (where appropriate).

3. Scope

The Ghana Health Service GHS recommends the use of CCTV at the following:

- Head Quarters level
- Regional Health Administrations
- District Health Administrations
- Hospitals and clinics

The areas to be covered are the

- Entrances and exits (gates)
- Parking lots and Garages
- Out Patient Departments (OPDs) waiting areas
- Records Sections
- Revenue Sections
- Stores
- Kitchen
- Pharmacy and
- Other critical areas that houses expensive equipment and other public access areas deemed important.

Note/Exemptions: Due to the associated privacy and confidentiality implications:

- Wards, consulting rooms, treatment rooms, theatres and recovery wards are exempted from CCTV coverage.
- CCTV cover may not be required at administration, elevator and inside goods vehicles, unless it is deemed very important.

4. Type of CCTV Systems to Use in Health Facilities

CCTV systems differ quite markedly. There are cameras that transmit analogue or digital images, via cable or wireless links; recorder that record images in different ways with different implications for quality and many methods of storing and manipulating the images. However, irrespective of the type of CCTV system the mode of operation are very similar. The many different types of CCTV systems and their corresponding different capacities to meet a variety of objectives warrant the development of guidelines for users of CCTV in health facilities for standardization and effective implementation and regulation.

GHS recommend the use of stationary, unattended cameras and on-site CCTV recording devices. However, a facility may choose an analog or digital video system as their finance may dictate. This document therefore primarily addresses stationary, unattended cameras and on-site recording devices. It also addresses both analog and digital video systems. This document recommends practice provide criteria for

- CCTV coverage and fields of view at GHS facilities.
- CCTV camera criteria that represents a common viewpoint of international and local experts and that of other interest groups.
- The legal implications and how they should be addressed

This guideline is not intended to replace or take precedence over other regulatory requirements in the specific jurisdiction of the establishment to which these guidelines will be applied. The intent of these recommendations and guidelines is to optimize image quality to facilitate the identification of individuals and objects that are depicted.

GHS recognizes that for certain applications, the recommended practices or guidelines, as implemented by it, may be either more or less restrictive than those given in this document. For example, in cases where state regulations govern portions of a hospital's operations, the government regulations take precedence over these recommended practices or guidelines. Furthermore, this document does not specifically address employee theft or other internal security issues although some of the recommendations can be applied to those problems as well; the GHS Code of Disciple may apply in this case.

Exemptions:

GHS recognizes that facilities have unique aspects of their operating environments that may result in less than a complete implementation with every provision of GHS Security Recommended Practice. The application of the standards, practices or guidelines contained

herein is voluntary. However, any health facility that does not rely on CCTV to ensure security should have risk assessment report that preclude it from its use. Where the health facility excluded from the use of CCTV system, it may use an alternate means to achieve an equivalent level of security. The facility should to put into writing and forward to the DG why they cannot use CCTV in their facility. They should address the following:

- State why CCTV provisions cannot be fully met;
- Identify an alternate security provisions that fully meet their needs;
- Describe the alternate means to ensure that equivalent security is achieved; and
- Provide a reasonable basis (i.e., operating history or threat and vulnerability analysis) for why security is not compromised through the alternate means.

5. Prior Requirement for Installation of CCTV System in a Health Facility

4.1 Health facilities that choose to install CCTV systems should first of all do a full cost-benefit analysis. If the they may go ahead to install the system if the benefits outweigh the costs.

4.2 Prior to the installation of CCTV system in any health facility, there should be comprehensive assessment made. This Recommended Practice is intended to satisfy the following objectives:

- Help health facilities select placement locations of CCTV cameras at existing and
- Identify recommended CCTV camera coverage considerations and fields of view for different types of service areas/departments of the facilities.

4.3 Risk Assessment Considerations

Health facilities should evaluate risk using system-wide and asset-specific risk assessments as a guide in determining effective placement of CCTV cameras to maximize coverage.

System Wide Assessment refers to the security risk to their systems' assets and the surrounding environment. To determine specific health facility risks, rank the Service's assets, the security and risk management issues criticality for each specific location being considered.

A careful survey of the establishment in which the system will be installed must be completed and analyzed as an integral part of the total system design process. A site plan documenting the location and field of view of each camera in the establishment should be included as a part of this survey.

Upon installation, the system must be tested to confirm that images produced by the system as output are of sufficient quality to maximize the likelihood of identifying individuals or objects depicted therein. The purposes of the requirements are to increase the likelihood that images recovered from CCTV systems are sufficient to enable health officials to identify the people and objects of interest depicted therein.

4.4 CCTV camera coverage and field of view documentation

CCTV camera coverage and fields of view should be documented upon installation and continually monitored, evaluated and updated:

(a) As part of any updated security risk assessments or any new assessments for health facilities;

(b) Based on information from facility maintenance staff; and

(c) As operating conditions change (such as significant expansion of the facility)

5.0 Brief Information about CCTV Systems to Use in Health Facilities

This section of the document addresses CCTV systems in seven areas. These are:

1. System Design
2. Recording systems
3. Cameras
4. Media
5. System Maintenance
6. Retention of Recordings
7. Procedures for Evidence Handling/Preservation

5.1 System Design

A CCTV system may include cameras, a monitor on which to view the camera images, a recording device to capture selected images and software or a switching system to control the method of selecting and storing images. Depending on the location and situation, video camera systems may use an analog videocassette recorder (VCR), a digital video recorder (DVR), or a PC-based digital recording capture station to record images from the cameras. Critically, a means of retrieving and storing images must be incorporated into the system.

A CCTV system to record images ability will be of greatest assistance to health administration and law enforcement depending on multiple factors such as the choice and

placement of cameras and lenses, recorders, storage space, and compression schemes. These factors are not independent of one another, but must be coordinated with one another. For example, adding cameras to an existing system may require adjustments to the amount of storage or the rate at which images from each camera are recorded.

5.2 System Components

CCTV systems should include the following components, at a minimum: (1) a camera or cameras, moveable and/or fixed; (2) a monitor; and (3) a recording device, including the means by which the recording may be extracted from the device. Consideration should be given to any need for recording audio with the video from one or more cameras, and any legal problems unique to audio recording. Guidelines for recording devices are addressed immediately below and in Section 7, while cameras are addressed immediately below and in Section 8.

5.3 Monitors

A monitor should be included with every CCTV system so that system operation may be checked on a daily basis (see Section 9). Monitors capable of operating in an under-scan mode are strongly recommended since this capability permits the viewer to observe the entire field of view being recorded.

6.0 Positioning of CCTV Systems

Health facilities may have a variety of CCTV camera coverage and field of view needs based on risks identified through a security risk assessment.

Areas to consider are OPDs, exterior and/or interior parking lots and garages, entrances/exits (gates and doors) for the premises, work areas and service areas within an institution, interior corridors or common building hallways, critical areas that houses expensive equipment, stores, kitchen, pharmacy, other public access and concession areas deemed important and as stipulated below.

The CCTV cameras should be placed to view pedestrian and vehicular entrances and exits. They should provide coverage and field of view of the entrances, exits and the entire length of the passageway, including stairways, ramps and elevator lobbies to monitor activities. Where there are multiple entrances and exits they may require camera view at each location. Consideration should be given to bidirectional flow. CCTV cameras are to be

placed in such a manner as to observe and monitor certain locations to aid in maintaining safe and secure health environments for patients, staff, operations critical infrastructure and equipment and supplies.

Camera placement should be optimized to avoid obstruction by other structures and by foliage (if any). Cameras' fields of view should not be obstructed in any way. They should avoid obstructions such as structures, shelters, trees and vehicles. In the case of foliage, the size of the planting at maturity and seasonal changes should be used as a baseline.

Consideration should be given to ensuring adequate lighting is provided so that cameras provide the best image possible. However, the cameras should not be pointed directly at bright light sources such as picture windows, spot lights, etc. If bright areas cannot be avoided in a scene, cameras with backlight illumination or compensation adjustments are preferred to optimize the resulting image.

Care should also be exercised to ensure that cameras are not located in places in which they may be subject to tampering or accidental adjustments. Using components feature that concealed wiring and protection of the camera and lens assembly from weather and/or physical damage can minimize camera disabling and tampering.

6.4. Number of CCTV Cameras

The number of cameras needed for any given facility should vary depending upon the number of specific security needs of the facility and the recommended area(s) to be monitored. Each facility should have a sufficient number of cameras to provide an overview of the facility. The CCTV security system may include a single camera or multiple cameras. Consideration of CCTV camera equipment type should be based on GHS Equipment and Procurement recommendations and technical standards for the selection of the cameras, digital recording systems.

As a minimum, there must be at least one camera for every exit. These exit cameras should be aimed toward the interior of the facility, and each one should be located where it can obtain an unobstructed frontal view of the head and shoulders of every individual exiting the facility. The lenses on exit cameras should be configured to have a depth of field that extends from 3-feet to at least 10-feet from the camera in order to provide images of exiting individuals that are in focus. Exit cameras that have a depth of field extending from 3-feet to beyond 10-feet will have the added benefit of providing overviews of the interior and head-to-foot views of people as they enter and exit the facility. Cameras should be placed where they can record images with unobstructed views at each of the recommended areas of the facility.

There must be at least one camera at each OPD. Cameras should be adjusted to ensure that they are in focus at the location that a patient/client can be expected to stand. If a window or other security barrier is present, care must be taken to position the camera in a manner that minimizes reflection, glare, and other obstructions that can interfere with a clear view of the persons or objects being recorded. The camera lenses needed to achieve the fields of view are discussed in Section 8. Cameras that provide overviews of the interior and exterior portions of an establishment can be useful in an investigation, but cannot be relied upon to provide images suitable for identification purposes. Therefore, in these guidelines they are considered to be of reduced importance. However, if the combinations of the exit and OPDs cameras do not provide complete coverage of the specified interior of the establishment, then it is recommended that additional cameras be included for this purpose. If deemed necessary, exterior cameras intended to record images of vehicles should be placed to provide direct views of the vehicle, so that the license plate is clearly visible and legible. Additional exterior cameras covering wider fields of view can provide additional vehicle information.

Health facilities may find it useful to include monitored cameras as a part of their overall security strategy. The views from such cameras are not intended to be recorded, but provide employees with a means to view areas within a facility that would otherwise be out of employees' sight. Moveable dome and pan/tilt cameras can be used to provide additional room coverage through automatic alarm presetting and parking. Motion detection or door contact alarms can automatically initiate a camera preset providing a high-resolution view of the alarmed scene. This provides un-manned, additional target coverage. After a pre-determined time, the camera can return to a preset parked position or to a scanning pattern to cover site locations not viewed by the fixed devices. If the system contains a matrix switch with a joystick controller, a guard or observer can manually track a suspect giving a tightly zoomed, high resolution image of the suspect. Variable speed control and automatic focus are recommended to facilitate smooth target tracking. When in the parked position, the unit can serve as an additional fixed camera. Specific information regarding camera types and lenses is provided in Section 8.

These primary recommended areas of coverage and fields of view are means of access and egress. The objective for coverage is to maximize the effectiveness of CCTV coverage and field of view. The CCTV cameras should be placed to monitor pedestrian and vehicular entrances and exits, vending areas and passageways. Overview images of these areas are recommended for general observation and to detect problems such as criminal acts.

Images of the parking garage are recommended for general observation and to detect problems such as criminal acts. Complete overview images of all parking garage areas may be difficult to obtain, due to obstructions and support beams. So, camera placement should be optimized to avoid obstruction by other structures and by foliage (if any). In the case of foliage, the size of the planting at maturity and seasonal changes should be used as a baseline.

6.2 Elevator Coverage and Field of View

Each obscured elevator cab entrance may have a camera mounted with the intent to obtain full coverage and field of view of the elevator exterior and entrance to monitor health activity.

6.5.2 Restricted Area Entrances

Wards, treatment rooms, theatre and offices should not have CCTV coverage. However, cameras should provide coverage and field of view to monitor and identify entrances and access points to restricted rights of way or for other purposes deemed necessary.

6.5.3 OPDs including Records Areas

Cameras should provide coverage and field of view of the entire length and width of the platform and platform edge to monitor health activity.

6.5.4 Revenue Collection Sites

The CCTV camera should be placed to view the point of transaction. The cameras should provide a recognizable image of the person(s) involved in the transaction/interaction.

6.5.5 Concession areas

Cameras should provide coverage and field of view to monitor concession areas.

6.5.6 Other Critical Areas

Cameras should provide coverage of other locations identified as warranting security monitoring through the system-wide and asset-specific security risk assessments.

6.6 Lighting

Poor lighting is the most common factor that degrades the quality of video images. Adequate, balanced lighting should be provided in areas viewed by the cameras. Particular care must be taken to ensure that the dynamic range present in a scene does not exceed the capability of the camera to record it.

Strong backlighting or high contrast lighting may cause the face of a subject to be obscured in shadow, making identification of a suspect from the image difficult or impossible. Likewise, spotlights can create both shadows and highlights on faces, making it difficult to determine if observed tonal variations represent actual features, such as facial hair, or are merely a product of the lighting. ***The use of non-infrared, high dynamic range cameras and those capable of operating in low light conditions should be considered to help improve the image quality.*** As an example, ceiling-mounted fluorescent lighting that is well distributed throughout interior spaces would be preferred to the use of track-mounted spotlights.

Different light sources have different color temperatures that will affect the apparent color of objects within a scene. Tungsten lamps impart a reddish tint to objects in a scene, while fluorescent bulbs can impart a greenish tint. Likewise, sodium lamps can make objects appear more yellow than they actually are. Most color video cameras can be adjusted to compensate for this, and many perform this function automatically.

A color video camera is considered balanced for a particular reference white when a neutral white card is placed in the camera's field of view under normal illumination conditions and the red, green, and blue channels provide equal output levels. Therefore, interior color cameras should be balanced for white upon installation, and rebalanced if the type of lighting used is changed. Note, however, that since many health institutions will operate under conditions in which lighting is variable, white balance may not be possible at all times.

Infrared (IR) lighting can be used to provide improved low light performance for monochrome cameras. IR lighting is not supported by standard color cameras as they filter out the IR spectrum. If an IR sensitive video camera is used, law enforcement officers should be made aware of this because an IR sensitive video camera often reproduces clothing that appears to be dramatically different when compared to images of the same clothing that were recorded with a video camera that is not sensitive to IR. A more complete set of technical guidelines for lighting is provided in Appendix B.

6.7 Electrical Power

CCTV systems must be provided with adequate power. Backup power sources and surge protection should be included in the system design to ensure that recordings are preserved in the event of a power loss. Systems that require electrical power to preserve their recordings should have backup power sources sufficient to last for at least thirty (30) minutes, until either the system power is restored or the system is shut down in a manner that preserves the recording. Video processors such as DVRs should also automatically restart in a preprogrammed operation mode upon power-up from extended power outages. When a VCR or DVR with automatic restart is used, there must be an ON-OFF switch on the front of the recorder. This is to ensure that no data is lost following an incident that led to the recorder being purposely turned off to preserve the recording of the event.

CCTV systems should be placed on isolated circuits that are properly grounded to reduce interference and signal degradation. If the system is on a long power run, outdoors, or in an area prone to electrical storms, special protection devices to control power surges and nearby lighting strikes are strongly recommended.

6.8 Bandwidth

The bandwidth provided for the transmission of the video signal must be compatible with, and sufficient to meet, the resolution requirements listed below for the system's recording device. While bandwidth minimum standards do not guarantee acceptable video image quality, they do play an important part. To improve the likelihood of acceptable image acquisition, video cameras should have a signal bandwidth of at least 7MHz.

6.9 Signal to Noise Ratio

One major problem with picture clarity is noise. Electronic noise is present to some extent in all video signals. Noise manifests itself as “snow” or graininess over the whole picture on the monitor and subsequently on recordings. There are several sources of noise: poor circuit design, heat, over-amplification, external influences, automatic gain control, and transmission systems. Some video signal noise cannot be overcome in a reasonable manner. However, to improve the likelihood of acceptable image acquisition, video cameras should have a signal to noise ratio of at least 48 dB. Further, the line loss between each camera and the multiplexer or recorder that the camera is connected to shall not cause the signal to fall below 45 dB.

6.10 Recorder security

Steps must be taken to ensure the physical security and integrity of the system's recording device. Placement of the recording device in a restricted access location, such as a locked cabinet or room, is strongly recommended. Note that proper environmental controls must be implemented per manufacturer specifications. For example, VCRs require adequate airflow to prevent overheating. Policies should be in place to ensure that law enforcement can gain immediate access to the recorded images when necessary.

6.11 Recordings of Associated Text Information

Both analog and digital CCTV systems include the capability to associate text information, such as time, date, and camera ID, with the images recorded by the system. In some cases, transaction or personal information may also be recorded in association with image data. This is often accomplished by superimposing the text directly upon the images. Time, date, and camera information is useful in investigations and should be preserved. However, text that obstructs the view of subjects' faces or vehicles' license plates may hinder investigations and should be placed to minimize its effect on image content. Test recordings should be performed to ensure that this requirement is being met and that the information being recorded is accurate.

GHS recommends that digital CCTV systems be configured so that associated text information is unalterable and preserved as data records or files that are linked to the respective images. In such cases where time and date, transaction, or personal information is recorded in digital systems along with the image stream, it must be possible for law enforcement to recover the images separate from this information.

For analog CCTV systems, in which it is not possible to separate personal or transaction data from the images, systems must be configured to record this information for one (1) second or less for each instance (e.g., transaction) in which such data is required. If the text information is visible on the recorded video, then the text characters must be as small as possible while still being legible, and it must be possible to position the text anywhere on the screen to minimize the effect.

Each individual image and transaction data packet should have a time/date stamp associated with it. Whenever possible the time/date stamp should be generated as close to

the image source as possible. For example, when a camera is directly wired to the digital recording device at the same site, then time synchronizing the recorder is sufficient. However, when the camera is located remotely (in another location) and connected to the recorder via a Wide Area Network (WAN), then the image may be delayed in transit. In those cases, it is highly desirable to associate the time stamp with the image at the source sensor (the camera) instead of at the recorder. A time-tag image file is then transferred over the WAN to the recorder. The trend toward using Internet Protocol (IP) cameras will facilitate this process where the IP camera is capable of accepting time synchronization input. The GHS accepted standard for time synchronizing computers and all digital data devices is the Network Time Protocol (NTP). It is an open standard sponsored by the GHS/MOH Internet Engineers. This standard specifies an accuracy level of the time synchronizing device called the Stratum level. The Simple Network Time Protocol (SNTP) is another such standard. With the proliferation of Global Positioning Satellite (GPS)-based timing equipment, these time references are readily available for low cost. The use of an industry standard time synchronization protocol is recommended for large facilities.

7. Recording Systems

Recording systems used in CCTV systems should adhere to the following minimum standards:

7.1 Recording Resolution for Analog Recording Systems

(VCRs): Analog VCRs must record each image at a minimum line resolution of 240 visible lines. This resolution is typical of most VHS VCRs. The use of VCRs with higher line resolutions (e.g., S-VHS VCRs and tapes) is strongly encouraged, since this improves image quality.

7.2. Recording Resolution for Digital Video Recorders (DVRs)

The minimum resolution requirements for Digital Video Recorders (DVRs) will vary depending upon the media used to record the images. Some manufacturers quote digital resolution (pixels) in analog lines of resolution. For rough comparative purposes, a minimum digital resolution of 450 lines can be used for DVRs using digital video tape. DVRs using a hard disk or optical disk for storage must record each frame at a minimum resolution of 640 pixels in the horizontal direction and 480 pixels in the vertical direction4. If images are recorded in field mode, then each field must be recorded at a minimum resolution of 640 by 240.

GHS strongly encourages the use of higher resolutions than those described above whenever possible.

7.3 Compression

Compression is a process in which the size of a digital file is reduced.
Due to the large amount of information present in each second of video, most digital video systems use compression to reduce storage and transmission requirements.

Compression may be "lossless" or "lossy". In "lossless" compression information is not lost. In "lossy" compression, information is lost. If a file has only been saved using "lossy" compression, then it is not possible to recover all of the information in the original file.

In the event of an alarm-triggered mode (see Section 7.8), it is recommended that lossless compression be used to record the sequence of interest, if possible. If a system is incapable of lossless compression during the alarm mode (as well as at all other times), then in order to maximize the amount of information available to law enforcement, it is strongly recommended that the lowest possible amount of compression be used in recording files. Some manufacturers utilize proprietary compression formats that require the use of proprietary software in order to view the video sequences or images. Use of such software can prevent or hinder law enforcement from viewing or otherwise accessing these images. If such software is utilized, then steps must be taken to ensure that law enforcement will be able to access them when needed (see Section 10 and 12).

7.4 Time Lapse Recordings NTSC video records images at a rate of approximately 30 frames per second.

Each frame consists of two fields or images, producing an actual rate of 60 images per second.

Analog videotapes are usually recorded in one of three speeds – SP (Standard Play), LP (Long Play), or EP/SLP (Extended Play/Super-Long Play). A T-120 tape recording at SP speed will record for a period of 2 hours, while a T-120 tape recording at LP speed will record for a period of 4 hours, and a T-120 tape recording at EP/SLP speed will record for a period of 6 hours. Changing the recording speed from SP to LP to EP/SLP does NOT

change the rate at which images are recorded – it remains 60 images (fields) per second. Any recording made at a rate of 60 fields per second is commonly referred to as a "real-time" recording.

Time lapse recorders are capable of recording video at rates that are much lower than 60 images per second. This enables the recording of images over a longer period of time. For example, using T-120 tapes, a VCR set in SP mode will record 30 frames (60 images) per second for 2 hours. With a time-lapse setting of 24-hours, a T-120 tape will run for 12 times the normal two-hour tape length, and the VCR will record no more than 5 images per second.

Some analog time-lapse video recorders manufactured specifically for CCTV security applications are designed to record a higher number of fields per second in different time-lapse modes. For example, some "High-Density" video recorders can achieve record rates of more than 20 fields per second in 24-hour time- lapse mode. Likewise, digital video recorders may also be capable of recording at higher rates.

In order to meet GHS guidelines, CCTV systems must capture and record at least one complete field per camera per second; any rate lower than this may result in inadequate temporal coverage of events in the scene.

7.5 Switchers/Multiplexers

Establishments with more than one camera may choose to utilize a device that enables the recording of images from all of the cameras to a single recorder. The two most common devices used to do this are switchers and multiplexers. Switchers, as the name implies, alternate among multiple cameras so that the output of the switcher at any one time is the signal from a single camera. Systems in which the output of a switcher serves as the input to the recording device will record images from each camera in succession. The time that it takes for a switcher to return to the same camera is called the "camera interval." The reciprocal of this interval is referred to as the "camera refresh rate." Therefore, a camera interval of ½-second would correspond to a camera refresh rate of 2-times-per-second. A multiplexer takes the outputs from multiple cameras and adds an encoded signal that allows a picture from each camera to be viewed in succession (as with switchers) or simultaneously. The encoded signal is almost always vendor-proprietary, making it difficult to recover the recorded images without the proper hardware and software. Switchers, multiplexers, and similar devices are frequently used to generate multi-image

displays. Multi-image displays consist of a split screen that allows for the viewing of more than one camera image on the screen simultaneously. Recording images in this mode, however, significantly decreases the individual camera's image size and quality. Many brands of duplex multiplexers will allow the user to view multiple camera images simultaneously, while still recording full-size images from each camera.

In order to meet GHS guidelines, CCTV systems **must not record** in multi-image modes. Given the requirement in section 7.4 that recordings capture at least one complete field per camera per second, this will restrict the refresh rate for each camera in a system with one recorder.

7.6 Triggers/Incident Recorders

In some situations, systems may include triggers that lead to the recording of images at a rate, or in a sequence, that differs from the normal operating mode. An example of this would be to change from time-lapse mode to real-time mode when triggered by an alarm button. Another example would be to include an otherwise inactive camera in the recorded sequence if motion was detected in the field of view of that camera. If such a device is used, its use **must not** conflict with the recommendation provided above in Section 7.4 (i.e., one field per second from every camera in the system must continue to be recorded at a minimum). Furthermore, test recordings should be made to ensure that activation of the trigger and subsequent operation of the incident recorder does not have a deleterious effect on the quality of the recorded images.

7.7 Remote Recording Some CCTV systems transmit the system signal (images and other information) to a remote site for recording.

The images transmitted this way are usually compressed significantly in order to meet bandwidth restrictions. As noted in Section 7.3, excessive compression severely degrades image quality. In those situations in which remote monitoring is practiced, GHS strongly recommends that recording devices also be installed at each monitored location, so that images may be stored with a minimum of image compression, when necessary.
In some cases, a remote facility recording video signals from multiple off-site locations may also have the capability to control recording devices installed at each off-site location. It is important to ensure that this capability be tested on a regularly scheduled basis. Procedures must be established that define the response by personnel at the remote facility

in the event of an incident at one of the off-site locations. Steps should be taken to preserve the recorded video at both the remote facility, as well as the off-site facility.

7.8 Alarm-Triggered Digital Buffers

In an alarm-activation event, law enforcement will seek to have the highest possible image quality. This includes recording images using lossless compression. Therefore, in order to meet GHS guidelines, CCTV systems that record images using lossy compression **must** have an alarm-mode included in their system.

Furthermore, in the event of an alarm trigger, in order to meet GHS guidelines, the following system settings are required for the alarm sequence:

1. Lossless compression;
2. The recorder must have a buffer capable of retaining the five (5) minutes of data prior to the alarm-trigger using lossless compression;
3. The system record at a rate of 60 fields per second, while maintaining the same rate at which the system switches between cameras (i.e., more pictures per camera each second if time lapse mode is normally used);
4. Once triggered, the system should continue to record in a lossless manner until manually stopped by user intervention by an authorized agent, per the establishment's policies and procedures5. This period of time should extend for at least 5 minutes after the completion of the crime or event that led to the alarm. The recorder shall have sufficient storage to be capable of recording in this mode for a minimum of 30 minutes.
5. All alarm data may be stored as black and white images.

Note: Any installed systems that are incapable of lossless compression should be configured to record the alarm sequence at the lowest possible compression ratio.

7.9 Digital Recorder Output Devices

Digital recording systems that do not use removable media for day-to-day storage must be capable of exporting exact duplicates of their recordings to removable media in a standard health format. This is necessary so that law enforcement officials can obtain copies of the recorded digital files that are a bit-for-bit copy of the files stored on the system.

In order to meet GHS guidelines, CCTV systems using digital recorders must be configured to permit output to write-once storage devices including compact disk (CD-

ROM). It is strongly recommended that systems also be configured to permit output to digital versatile disk (DVD). This latter recommendation is based on the observation that the recording of any alarm-triggered event will be over 10 minutes in length (5 minutes before the alarm, plus the duration of the event, plus 5 minutes after the event). The greater storage capability of DVDs will reduce the number of disks needed to store the recording on removable media. Systems designed to output to DVD should **not** utilize standard compression techniques used in the production of consumer DVDs, but should be capable of making bit-for-bit copies of files recorded on the system hard drive(s).

Note well!!

- Facilities operating CCTV systems should ensure that, the Systems are configured to stop recording in the event that the recorder runs out of memory/storage space prior to user intervention, in order to retain the existing images.

- GHS recommends that all facilities ensure at all time that soft copy evidence is provided to law enforcement using media that requires no special hardware, but represents an industry standard. This can be in the forms of CDs , DVDs or other types of media.

7.10 Output File Types

Digital recording systems must be capable of exporting exact duplicates of their digital image files to removable media. If a system utilizes a proprietary format to store images, then steps must be taken to ensure that law enforcement can extract an exact copy of each image in the recording in a lossless and open file format capable of fully supporting the recorded data. The current preferred file format for such applications is TIFF.

Furthermore, in order to assist law enforcement in the expeditious dissemination of still images immediately after an event, digital recording systems must be capable of directly exporting still images at the highest quality setting in one of the following industry standard formats: TIFF, BMP, or JPG. The ability to export to an uncompressed non-proprietary AVI file and the native video file format, in addition to one of the previously mentioned still image formats, is desirable as well. All output formats must maintain accurate aspect ratios consistent with the original recording. See Section 11 for further information regarding guidelines for output in the event of a criminal incident.

8 CCTV Cameras Equipment

Consideration of CCTV camera equipment types should be based on GHS Recommended Practice; Technical Standard for the Selection of Cameras and Digital Recording Systems. It is the position of the GHS that in order to optimize the use of these systems the following criteria should be met:

1. The number, placement, and type of cameras should be sufficient to provide adequate coverage and detail in the monitored area.
2. Adequate, balanced lighting should be provided in the monitored area.
3. Facility should establish and follow a program of regular maintenance for their systems.
4. Facility should have documented procedures to ensure that employees know what to do in the event of a criminal incident.
5. Recordings that depict criminal activity must be preserved in a manner that permits law enforcement officials to recover the original images with a documented chain of custody.

Cameras used in CCTV systems should adhere to the following recommendations:

8.1 Black and White vs. Color Cameras.

Although black and white video cameras may provide better image resolution than color cameras, the information available in color images may provide important investigative information. Therefore, the choice of cameras is left to the health institution, dependent upon the intended use of the recorded images.

8.2 Camera Detector Size

Video and digital cameras use detectors that come in a variety of sizes. Typical sizes are 1/4", 1/3", and 1/2". The size of the detector will have a direct impact on the focal length of the camera lens. See Section 7.5 for further information.

8.3 Camera Resolution

In order to meet GHS guidelines, analog video cameras must have an output resolution of at least 400 horizontal lines. Digital video cameras MUST have an output resolution of at

least 480 horizontal lines. GHS strongly recommends that cameras that have higher resolutions are used.

8. 4 Camera Infrared Characteristics

The detectors used in black and white video cameras may be sensitive to a part of the infrared spectrum that is outside of the normal range of human visual perception. This can improve the ability of the camera to record in low-light situations. Due to the fact that images acquired by infrared-sensitive cameras can make some dark clothing and other objects appear to be lighter than they actually are, it is recommended that infrared-sensitive cameras not be used to record scenes that are well-illuminated. Many cameras are equipped with filters that can mitigate this effect. This does not apply to most color cameras that normally contain an infrared barrier filter to block infrared light. The use of infrared-sensitive cameras should be noted within the system documentation (see Section 10.1).

8.5 Lens, Focal Length, and Field of View

In order to identify a person, one must be able to distinguish specific individual features on a person such as the detailed shape of the eyes, ears, nose, mouth, and chin. Identification is facilitated if one has the ability to distinguish smaller features such as tribal marks, moles, scars and any physical marks/ patterns, as well as the ability to derive measurements of these features. Similarly, identification of a vehicle will require that one be capable of objectively reading the license plate numbers, or distinguishing other identifying characteristics.

Therefore selection of lenses should be determined by the field of view to be covered by each camera, as well as by the size of the camera's detector. For cameras placed to record images at OPDs, car parks and the area of interest (face, license plate, etc.) should cover approximately 15% or more of the camera's field of view (based upon the recommended minimum resolution found in Section 7.3). For an average human head that is 6-inches wide, a 3-foot-wide field of view will meet this guideline. For a license plate width of approximately 12-inches, a 6-foot-wide field of view is sufficient.

Cameras that provide overviews of interior and exterior locations should have their focal lengths selected so as to meet the field-of-view requirements of the establishment. Note,

however, that exit cameras should have sufficient depth of field to be in focus at distances of 3-feet and beyond to ensure that subjects exiting the facility will be in focus.

8.6 Exposure Control

Cameras should be equipped with automatic mechanisms to ensure proper exposure under varying lighting conditions. Such mechanisms include, but are not limited to, automatic gain circuitry, day/night sensor switching, and lenses with automatic iris functions.

8.7 Camera Housings

Cameras may require coverings and environmental controls to protect them from the elements or tampering. Note that clear coverings placed in front of camera lenses will reduce image quality. Therefore, unless there are specific environmental or security concerns that require camera housings, it is recommended that they not be used.

9. Media

Media, including analog videotapes, compact discs, digital video tapes, and DVDs, should be of high quality and meet equipment manufacturers' specifications. Low quality media can result in damaged equipment and poor images.

10. System Maintenance

CCTV systems should be maintained in a manner that ensures their proper function over their entire lifetime. Therefore, the following recommendations should be followed:

10.1 Documentation of System

Institutions should maintain documentation regarding their CCTV systems that include the following information:

1. Make and model of all system components, including recorders, cameras, lenses, and multiplexer/switcher, etc. For digital systems, this information should include software and hardware information, including software version. If infrared-sensitive cameras are in use, their location should be documented. An example of a system information sheet is included in Appendix C. If possible, a photocopy of the maintenance record should be included.

2. Adequate system documentation should be included at the site. This includes instructions for downloading and outputting recordings.
3. Point of contact information for system installer and/or system maintenance organization, to include at least two names and telephone numbers.
4. Site plan showing all equipment placement (including recorders), as well as field of view for each camera. Appendix C includes an example of a site plan. This information should be verified monthly and made available to responding law enforcement officials upon their arrival at the scene.

10.2 System Validation and Maintenance

Prior to use, systems must be validated to meet the requirements of Section 5 and 6 – to which they must be capable of acquiring, recording, and producing output images that are of sufficient quality to enable law enforcement officials to identify the people and objects depicted therein.

- Revalidation of these requirements must occur every time the system is altered.
- A variety of system checks and maintenance are necessary at different times.
- If system errors are found, steps to correct them should be implemented.
- A maintenance log must be maintained to document all system validation activities, checks and maintenance activities.

Review live images from each camera to ensure this: Are the times and dates correct? How one does this will depend upon the system design. Is the removable recording media (i.e., tape) properly installed and in the record mode? Check that the record indicator is active and that the tape counter is advancing.

Activities to Check Daily

Is the system secured? Check physical locks on cabinet and/or doors. Clean lenses and camera housings. (Care must be taken to avoid damage and misalignment.) More frequent cleaning may be necessary depending upon environmental conditions. Follow manufacturer's specifications. For systems using removable media (i.e. tape) recording mechanisms should be cleaned. Follow manufacturer's specifications.

Activities to Check Monthly

Check environmental controls (temperature and humidity) to ensure that they meet manufacturer's specifications for all system components. Follow manufacturer's specifications. Complete system preventive maintenance check. A qualified CCTV

technician should perform this check. For digital systems using hard drives for storage, a check for bad clusters and other disk errors should be performed. Refer to manufacturer instructions and specifications.

Ensure written policies and procedures regarding system operation are up to date. Review existing policies and procedures and revise as needed. Ensure employee competence in system operations, including alarm-mode response.

Conduct Operator Training.

Ensure system output to compact disk meets law enforcement needs. Write sample images from system to removable media and review images on separate computer system.

10.3 Frequency

These should be done annually:

- Ensure that reusable media is replaced. This is to be performed by system Operator Section 10.3
- Maintenance of recording media facility requirements should dictate the length of time for which recorded images must be archived.
- All recording media has an expected usable life span. Based on that life span, policies should be developed to ensure that media is replaced before this period expires. For example, VHS video tapes should be reused no more than 12 times and that they are replaced on an annual basis. Note that use of extended time-lapse mode may drastically shorten the life span.
- For digital recording devices, manufacturer's recommendations for maintenance and the device service life replacement schedule should be observed.
- A regular ongoing (automated) inspection of hard drives should be conducted to ensure that the disk(s) is/are functioning properly and that there are no bad sectors or other hardware errors that could result in a loss of data.
- Other reusable media must be re-certified no less frequently than the manufacturer's guaranteed period.
- Facility should establish policies regarding the marking of removable media so that the most recent date of recording will be documented.

11. Retention of Recordings

The purpose of this section is to provide guidelines regarding the retention of recorded media. It is recommended that analog videotapes be retained for a minimum of thirty-one (31) days before being reused. This coincides with the twelve-time use recommendation. For ease of retrieval, each videotape should be sequentially numbered and the dates and times recorded on each tape should be written on a label on the videotape. Due to the nature of digital recordings, the GHS recommends that recordings be retained for the longest time possible (minimum of 10 days) with the least amount of compression available within the system's capabilities. Storage capacity to meet these needs must be considered.

12. Evidence Handling Procedures

This section addresses procedures to follow when law enforcement response is necessary. This may be in response to a robbery, or it may be related to other criminal investigation.

12.1 Documentation for Law Enforcement

The system documentation, as described in Section 10.1, including equipment information, site plan, contact information, and maintenance log should be made available to responding law enforcement officials. Any additional pertinent information regarding the recording or the incident itself should be noted, such as incident time, record mode, discrepancies between actual time and recorder time. Appendix C includes an example of this type of documentation.

12.2 Handling of Evidentiary Recordings

Following an incident involving immediate law enforcement response, it is necessary to ensure that the recorded images are secured. Unless the possibility exists that the images may be over-recorded or overwritten, the recording should not be stopped until the arrival of law enforcement officials.

12.2.1 Video Cassette Tape Systems

Upon termination of recording, the tape should be removed from the recording device and the recording tab immediately removed or shifted to the record disabled setting. The tape should not be played again prior to the arrival of law enforcement officials. The name of the institution and identity of the individual performing this function should be marked on the exterior of the cassette housing, along with the time and date of removal. Prior to transfer to law enforcement officials, steps must be taken to ensure that the tape is not mishandled or damaged. This includes keeping the tape away from magnetic fields, such as those generated by televisions, radios, and speakers. Steps should also be taken to keep the tape at room temperature and out of direct sunlight.

Tapes should not be stored for an extended period of time. Personnel qualified to assist law enforcement in the recovery of images from the tape should be identified and made available prior to the arrival of law enforcement officials.

12.2.2 Digital Video Systems

The following steps should be followed:

1. Upon termination of recording, personnel qualified to assist law enforcement in the recovery of images from the CCTV system should be identified and made available to offer technical assistance. This representative shall be available either in person or via telephone.

2. Law enforcement officials will coordinate with appropriate personnel to view and retrieve the best image(s) prior to the officials' departure from the crime scene. When immediate transmission of images is necessary to expedite distribution from the crime scene, they should be transmitted via network, E-mail, compact disk, or other available means. Images shall be provided to law enforcement in the TIFF, BMP, or JPEG format. If the establishment utilizes a remote location for the storage of recorded images, then the establishment will provide the images to an address designated by the law enforcement officials.

3. The establishment's security personnel will produce at least two copies of the relevant images and video on CD or DVD (non-rewritable) in the non-proprietary formats as well as the original native format.

4. In the event of alarm-trigger incidents as described in Section 6.8, law enforcement would like all video and relevant data that were recorded five minutes before the

alarm-trigger, the entire incident, and five minutes after the incident. This is barring any outside circumstances when it is required to save a longer period of time, i.e., a casing of the bank, etc.

Appendices

a. Appendix A – Facility Risk Assessment Tool

b. Appendix B – Technical Guidelines for Lighting

In this document, luminance is measured in Lux. Some older documents and references may refer to the measurement in foot candles. 1 foot candle is equivalent to 11 Lux. To provide good quality camera images, a minimum of 275 – 333 Lux of illumination should be provided in the patient/client areas, office areas, hallways, stairways and exits where camera coverage is provided.

Exterior self-service facilities, such as ATM vestibules or drive up lanes, should have a minimum of 110 Lux of illumination 24 hours per day to ensure good image quality. Exterior areas such as sidewalks, entrances, night depository areas, etc. that are provided with camera coverage should be provided with a minimum of 55 Lux of illumination. Parking lots provided with camera coverage should have a minimum of 11 Lux of illumination at ground level. Supplementary surface lighting may be necessary to provide adequate illumination for the face of anyone using any Revenue or Concourse resource.

c. Appendix C – System Documentation And Site Plan Examples System Equipment Information:

1. Recorder Make and Model
2. Multiplexer Make and Model
3. Camera/s Make and Model
4. Are any cameras infrared-sensitive, and if so identify them
5. Video Format (circle) VHS SVHS DVR (Digital Video Recorder) PC

d. Appendix D – Other

If Digital Video Recorder or PC-based:

1. Hardware Manufacturer
2. Software Name and Version
3. Is a copy of the most current maintenance/service log attached? (circle) Yes/No
4. Does the system record multiple cameras? (circle) Yes/No

    a. If yes, how many?
5. Contact Information:
    a. Point of contact for recording system:
    b. Contact's name and phone number:
6. Point of contact for facility:
    a. Facility name phone:
7. If system records multiple cameras, note camera location and Angle view
8. Law Enforcement response:
9. What record mode was the system in? (circle) 2 Hours 6 Hours 12 Hours 24 Hours 48 Hours 72 Hours

e. Other Unknown

1. Does the recorded date/time accurately represent the time of day? Yes/No (circle)
2. Note date/time of incident
3. Note date/time of incident on tape
4. Note date/time recording removed from equipment
5. Any other Information:

GHS Data Protection Policy

1.0 Introduction

This document sets out the appropriate actions and procedures, which must be followed to comply with the GHS Data Protection Policy in respect of the use of CCTV surveillance systems managed by GHS. In drawing up this policy, due account has been taken of the following:

1. MOH/GHS data Protection Policy …..;
2. The Data Protection Ghana Bill 2010;
3. The CCTV Code of Practice produced by the Internal Standards (International);
4. The Human Rights Ghana Act …..;
5. GHS Code of Ethics 2002;
6. GHS Code of Conduct and Disciplinary Procedure 2003

An important new feature of the legislation is the CCTV Code of Practice which sets out the measures which must be adopted to comply with the Data Protection Policy, Act …. This goes on to set out guidance for the following of good data protection practice. The code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place.

2. Scope

This policy will cover all employees of GHS, persons providing a service (voluntary or paid) to the Service, patients, visitors and all other persons whose image(s) may be captured by the system.

3. Definitions

3.1 Prior to considering compliance with the principles of the Data Protection Policy, a user of CCTV or similar surveillance equipment, will need to determine two issues:

3.2. **The type of personal data being processed.** That is, is there any personal data which falls within the definition of **sensitive personal data** as defined by the documents mentioned above 'Sensitive personal data' includes:

- Gender;
- Ethnic origin or race
- Political opinion;
- Religious beliefs;
- Professional Association Membership
- Trade Union membership;
- Health – mental or physical;
- Sexual life;
- Commission of any offence (or alleged);
- Any court proceedings or findings;

3.3 The **purpose(s)** for which both personal and sensitive personal data is being processed. The data must be:

- fairly and lawfully processed;

- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary
- processed in accordance with individual's rights;
- secure;
- not transferred to countries without adequate protection;

3.4 The Health Information Department will take into account the extent to which users of CCTV and similar surveillance equipment have complied with this Code of Practice when determining whether they have met their legal obligations when exercising their powers of enforcement.

4.0 Policy Application

4.1 Initial Assessment Procedures

4.1.1 The Head of the facility has the legal responsibility for the GHS CCTV systems. However, the Service's Security Manager has responsibility for the day-to-day compliance with the requirements of the CCTV Code of Practice.

4.1.2 The purpose of the facility's CCTV scheme is for the:

- Prevention or detection of crime or disorder;
- Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings);
- Interest of public and employee Health and Safety;
- Protection of public health;
- Protection of facility property and assets.

4.1.3 Prior to any camera installation the Security Service Company will have to ensure that the installation complies with the GHS Data Protection Policy and CCTV Code of Practice.

4.2 Siting the Cameras

4.2.1 It is essential that the location of the equipment be carefully considered, because the way in which images are captured will need to comply with the Data Protection Act.

4.2.2 All cameras are located in prominent positions within public and staff view and do not infringe on clinical / treatment areas. All CCTV surveillance is automatically recorded and any breach of these Codes of Practice will be detected via controlled access to the system and auditing of the system.

4.2.3 Signs have been erected on all entrance points to Service premises and throughout the site to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. The signs must include details on the purpose, organization and contact details.

4.2.4 Use of Covert CCTV (Directed) surveillance if required should be requested through the Minister of Health/the Director General/Police. If the request through the police is refused then authority can only be given by the GHS Security Management Service. This is covered by the GHS Data Protection Policy

4.3 Quality of the Images

4.3.1 It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme be clearly identified. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

4.3.2 All camera installations and service contracts should be undertaken by approved security companies. Upon installation all equipment is tested to ensure that only the designated areas are monitored and high quality pictures are available in live and play back mode. All CCTV equipment should be serviced and maintained on an annual basis.

4.3.3 All the system cameras, recording to digital recording media are currently monitored at the Facility Head's Desk/Office with recording and monitoring facilities elsewhere within the facility.

4.4 Processing the images

4.4.1 Images, which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the GHS Policy.

4.4.2 Where the images are required for evidential purposes in legal or the Service disciplinary proceedings, a CD-R disc recording is made and placed in a sealed envelope signed and dated and held by the Security Manager until completion of the investigation. Viewing of images within the security Office is controlled by the Security Manager or a person nominated to act on his behalf. Only persons trained in the use of the equipment and authorised by the Security Manager can access data.

4.5 Access to and disclosure of images to third parties

4.5.1 It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled. This will ensure that the rights of individuals are preserved, but also to ensure that the continuity of evidence remains intact should the images be required for evidential purposes e.g. a Police enquiry or an investigation being under taken as part of the Trust's disciplinary procedure.

4.5.2 Access to the medium on which the images are displayed and recorded is restricted to Service staff and third parties as detailed in the purpose of the scheme.

4.5.3 Access and disclosure to images is permitted only if it supports the purpose of the scheme. Under these conditions, the CCTV images record book and the appropriate view / release form (Appendix 1) must be completed.

4.6 Access to images by individuals

4.6.1 Any individual implicated by the video recording has the right to request access to CCTV images.

4.6.2 Individuals who request access to images must be issued an access request form (appendix 1). Upon receipt of the completed form, the Security Manager and the

Service's Data Protection Officer will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged then the request can be refused.

4.6.3 A written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons) within 21 days of receipt of the enquiry. If disclosure is appropriate, a payment in advance of the current approved fee will be required.

5.0 Interaction with Other Services, Policies and Procedures

This policy should be read in conjunction with the Service's Data Protection Policy.

6.0 Responsibilities

6.1 The GHS Board has corporate responsibility for the implementation of this policy, monitoring its effectiveness and ensuring the CCTV Code of Practice is available on the Service's website http: //www. ghs.org/ICD or from the Service's Security Service Company.

6.2 The Service's Council discharges this responsibility through the Director General and Director ICD and Head of Estates and/or facilities Head to whom the Service's Security Manager is accountable.

6.3 The Service's Data Protection Officer is also personally accountable for ensuring that the policy and Code of Practice are adhered to and monitored.

4. References

This Recommended Practice should be used in conjunction with the following:

- CCTV camera original equipment manufacturer (OEM) specifications;
- GHS policies and procedures for placing, maintaining and inspecting CCTV cameras; and
- Other related Security Standards, such as GHS Equipment Standard for CCTV Inspection, Testing and Maintenance.

7.0 Enforcement

The Information Department/ICT has the power to issue Enforcement Notices where they consider that there has been a breach of one or more of the Data Protection Principles. An Enforcement Notice would set out the remedial action that a Committee requires of the Service to ensure future compliance with the requirements of the Policy.

8.0 Documentation

Copies of all documentation and records relating to the CCTV system should be held within Security Department and the GHS Data Protection Officer and shall be kept under restricted confidentiality, for a period of 6 years.

9.0 Review

This policy will be reviewed every two years, or earlier in the light of changing circumstances by the Security Steering Committee.

Appendix 1

GHS Access to View or Copy Images by Police should have:

1. Full name of person making request:
2. Organization:
3. Address:
4. Telephone Number(s):
5. Date:

Form for details of Image to Be Viewed shall include:

1. Date:
2. Reason: (For police only)
3. Signed:
4. Dated:
5. Request Granted:
6. Request Denied (with Reason):

Form to Be Completed If Images Are Removed shall have:

1. Ref. No.

2. Issued To:
3. Crime No: (For police only)
4. Date Issued:
5. Issued By:
6. Return Date:
7. I acknowledge receipt of the above CD:
8. Signed: Date:

Application Form for Access to CCTV Images under the GHS Data Protection Policy

GHS uses CCTV systems for the purposes of crime prevention, the prosecution of offenders and public safety. The Data Protection Policy gives one the statutory right of access to the CCTV images we process about you. Please complete this form if you wish to access a CCTV image.

If you require assistance, please contact:

The Data Protection Officer or
The Head, Clinical Services Development Department
Institutional Care Division
Ghana Health Service, Head Quarters
Accra

Timescale

On receipt of your completed form and fee, we will respond to your request promptly, and in no more than 40 days. If we encounter any difficulties in locating your image(s) we will keep you informed of our progress.

Submission of Form

Please return this form to the Data Protection Officer at the following address:

The Data Protection Officer or
The Head, Clinical Services Development Department

Institutional Care Division
Ghana Health Service, Head Quarters
Accra

Notes To Assist In Completion of the Form Location (Note 1)

Provide details of the camera location, and the date and time of the image(s) you would like to see, as well as a general description of your appearance, clothing etc at the time in question.

Declaration (Note 2)

The person making the application must complete this section.

1. If you are the data subject- tick the first box and sign the authorization then proceed to Section
2. If you are completing this application on behalf of another person, in most instances, we will require their authorisation before we can release the data to you. The data subject whose information is being requested should be asked to complete the 'Authorisation' section of the form. (Section 5)
3. If the data subject is a child i.e. under 16 years of age the application may be made by someone with parental responsibilities, in most cases this means a parent or guardian. If the child is capable of understanding the nature of the application his/her consent should be obtained or alternatively the child may submit an application on their own behalf. Generally children will be presumed to understand the nature of the application if aged between 12 and 16. However, all cases will be considered individually.

Applicant (Note 3)

The applicant is the person who is applying on behalf of the data subject to get access to the CCTV image(s).

Countersignature (Note 4)

Because of the confidential nature of data held by GHS it is essential for us to obtain proof of your identity and your right to receive CCTV image(s). For this purpose it is essential

that your application should be countersigned by any one of the following: a Member of Parliament, Justice of the Peace, Minister of Religion, a professionally qualified person (for example, Doctor, Lawyer, Engineer, Teacher), Bank Officer, Established Civil Servant, Police Officer or a person of similar standing **who has known you personally for a period of 2 years**. **A relative should not countersign.** The responsibility of the Services' Data Protection Officer includes a check to confirm that the countersignature is genuine. In certain cases you may be asked to produce further documentary evidence of identity. The person who countersigns your application is only required to confirm your identity and witness you signing the 'Declaration' There is no requirement for this person to either see the contents of the rest of the form or to give any assurance that the other particulars supplied are correct.

Request For CCTV Image Subject Access Under GHS Data Protection Policy

You are advised that the making of false or misleading statements in order to obtain access to personal information to which you are not entitled is a criminal offence.

Section 1: Data Subject Details

Please supply a photo to aid in identification:

1. PHOTO
2. Name:
3. Date of Birth:
4. Sex:
5. Address: Home Telephone No:
6. Work Telephone No:

Section 2: Location (Note 1)

1. Date Area Approx
2. Time
3. Description Of Clothing
4. etc

Section 3: Declaration Statement (Note 2)

This section must be signed in the presence of the person who certifies your application. I declare that the information in this form is correct to the best of my knowledge and that I am entitled to apply for access to personal data referred to above under. Please tick appropriate box

1. I am the person named (go to section 6)
2. Signature of Data Subject: ……
3. Date: ……

or

4. the terms of the Data Protection Policy.
5. I am the agent for the person named and I have completed the authorisation section
6. I am the parent/guardian of the person who is under 16 years old and has completed the
7. authorisation section
8. I am the parent/guardian of the person who is under 16 years old and who is unable to understand the request (go to section 6)
9. I have been appointed by the Court to manage the affairs of the person (go to section 6).

Section 4: Applicant Details (Note 3)

1. Applicants Name (please print)
2. Address to which reply should be sent (if different from over)
3. Signature of Applicant

Section 5: Authorisation Statement

1. I hereby authorise South Devon Healthcare GHS Trust to release CCTV images they may hold relating to me to Enter the name of the person acting on your behalf) to whom I have given consent to act on my behalf.
   ……..
2. Signature of Data Subject Date .....

Section 6: Countersignature (Note 4)

To be completed by the person required to confirm the applicant's identity

I (insert full name) .....

Certify that the applicant (insert name).....

Has been known to me as a (insert in what capacity eg employee, client, patient etc) .....

For _____ years and that I have witnessed the signing of the above declaration.

1. Name: (*please print)*
2. Profession:
3. Address:
4. Telephone Number:
5. Signature:
6. Date:

Official Use Only

1. Date Request Received Amount Paid
2. Date Form sent to applicant
3. Method of Payment
4. Date Form Returned Date sent to System
5. Administrators
6. Certification Checked Data checked
7. Date completed