2006

Electronic surveillance in hospitals: A review

Sue Kennedy
Edith Cowan University

Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

Electronic surveillance in hospitals: A review

Sue Kennedy
Edith Cowan University
Western Australia
email:s.kennedy@ecu.edu.au

Abstract

This paper focuses on the increasing use of electronic surveillance systems in hospitals and the apparent lack of awareness of the implications of these systems for privacy of the individual. The systems are used for identification and tracking of equipment, staff and patients. There has been little public comment or analysis of these systems with regard to privacy as their implementation has been driven by security issues. The systems that gather this information include video, smart card and more recently RFID systems. The system applications include tracking of vital equipment, labelling of blood and other samples, tracking of patients, new born babies and staff. These applications generate a vast amount of digital information that needs to be correctly secured to protect the privacy of the individual. Separately each type of information has value, but if this information were analysed together then the intelligence that can be gleaned from this could become a major threat to privacy and security. There are various standards and legislation that cover healthcare information, such as CCTV, but are these known and what are the compliance levels? RFID use is increasing in the hospital sector and this is being linked with the patient medical record as it is becoming core to treatment in some hospitals. The indications are that this will become normal practice which means that surveillance information from RFID systems will be linked much more closely to a patient's medical record. Managers, owners and custodians of information within hospitals need to be aware of the issues and take steps to ensure that staff are fully aware and trained in information handling practices. They also need to ensure that external parties who handle surveillance information are compliant with standards and good practice.

Keywords
Electronic surveillance, information security, privacy, ownership, RFID (radio frequency ID).

INTRODUCTION

Healthcare is an area that is continually seeking to improve the outcomes for its patients. This includes the areas of treatment, administration and safety. In recent years there has been an increase in the use of electronic surveillance systems. These systems cover diverse areas of the hospital and are introduced to reduce risk to patients, staff and visitors to the hospital (Aldridge, 2005). The systems that gather this information include video, smart card and more recently Radio Frequency ID (RFID) systems. The applications include tracking of vital equipment, labelling of blood and other samples, tracking of patients, new born babies and staff.

Despite the increased implementations of these electronic surveillance systems in hospitals there is an apparent lack of awareness of the implications of these systems for privacy of the individual. There has been little public comment or analysis of these systems with regard to privacy as their implementation has been driven by safety and security issues. The current climate of perceived terrorism-related threats has further reduced the likelihood of widespread questioning of the ethics of these systems (Australian privacy Foundation, 2005) as indicated by the Office of the Privacy commissioner's statement noting "that the use of CCTV technology raises significant privacy and civil liberties concerns which must be balanced with the Code's utility as a risk-based counter-terrorism and law enforcement tool." (The Office of the Privacy Commissioner, 2006).

These surveillance applications generate a vast amount of digital information that needs to be correctly secured to protect the privacy of the individual. Separately each type of information has value not only to the patient but also to others; for example, for marketing purposes (OCR HIPAA, 2003); but if this information were analysed together then the intelligence that can be gleaned from this could become a major threat to privacy and security, particularly as the ownership of this information is not always well understood.

This paper will describe the different hospital applications where surveillance is in use currently, the reasons for the surveillance, the different types of surveillance in use and the implications of the surveillance to privacy and security.

HOSPITAL AND HEALTHCARE PRIORITIES

As suggested in the "model hospital mission statement" (Bart and Hupfer, 2004), the core business of a hospital should be "to arrest and eliminate disease and illness wherever possible, to become the most admired hospital in our industry and to provide an organizational climate in which honesty, openness, teamwork and innovation dominate everything that we do". In order to do this they need to protect and treat the patients in a way that will not be detrimental and hopefully will improve their state of health.

New technologies can assist by reducing the delay in treating a patient, reducing errors in treatment, locating vital equipment and medical staff in a timely manner, tracking samples, test results and the patients themselves (Collins, 2004). Different areas of the hospital use surveillance and tracking for various purposes; the main ones are described here.

Treatment

The administration of incorrect drugs, incorrect dosage, or blood of the wrong type, potentially could cause harm or death to the patient (National Patient Safety Agency, 2004). Increasingly, all this information is available electronically and can provide faster and more accurate treatment. However, this is only possible if the identity of the patient is accurately determined (Collins, 2006). In many hospitals worldwide a non-electronic wristband is the normal method used to provide this identification and it is then manually linked with the patient's records, which can leave room for error. Using an electronic identifier minimises the margin for error and can reduce the risk of mistreatment of a patient (National Patient Safety Agency, 2004).

Administration

Hospital administration covers a large number of varied areas including all the normal business functions such as financial management and accounts, HR, marketing, purchasing, risk management, audit, IT, maintenance, etc. It also includes functions specific to the healthcare industry such as medical and nursing services, bed occupancy, room and board, laboratory, radiology, pharmacy, appointments and laundry, to name just a few of these services. A patient may be charged for some or all of these services depending on the nature of the hospital and the services rendered. Computerised systems are used to track, record and bill for these services. An electronic identifier can be used not only to ensure that the patient is receiving the correct treatments but also to ensure that the correct patient is billed appropriately (Evans, 2006).

Security

Hospitals have many areas that are open to the public. They have a duty of care to all patients to ensure that they are protected from other patients, visitors and any other individual (or group) that might threaten them. People are at their most vulnerable when sick or injured and, at that time, may not be capable of lucid thought or appropriate action. Staff also need protection as they work in an environment that requires them to deal with patients and/or visitors who may be unreasonable, incoherent or intoxicated 24 hours a day (Aldridge, 2005). Therefore, the use of restricted areas, CCTV of public areas, access control and RFID identification for staff, patients and new born babies has become more common.

Privacy

Organisations in Australia are covered by the Federal Privacy Act (Privacy Act 1988 (Cth) s. 95A). Since December 2001 health service providers are required to comply with the Federal Privacy Act and the National Privacy Principles (Crompton, 2001). This also covers doctors and pharmacists. Since 2002 there have been a number of federal enquiries by the Australian Law Reform Commission and the Australian Health Ethics Committee into the privacy issues relating to the human genetic information (Australian Law Reform Commission/Australian Health Ethics Committee, 2002). Thus, health-related information must be protected to an adequate standard to meet the privacy requirements of the Act.

WHY SURVEIL?

In an environment that has so many areas open to the public, safety and security are harder to guarantee. Therefore, security measures need to be implemented to minimise the risks of an incident occurring. These measures can be used to help identify the perpetrator of an incident after the event. (They may also help avoid litigation if the hospital can prove due diligence.) (Aldridge, 2005).In order to do this it is necessary to be able to identify people and to track their movements when required.

Identification

It is essential in a hospital to be able to identify who is allowed into which areas. The reasons may be for safety, security or crime prevention. Safety reasons could be due to the risks associated with x-rays, radioactive materials, biological hazards, exposure to dangerous chemicals, highly infectious diseases, or patient vulnerability, such as in the case of a cancer patient with extremely low levels of white blood cells due to the cancer treatment (OSH Act 1970 (US). s.5A).

Security reasons could be related to violent patients, relatives or other visitors, health-related information and medical records, or the risk of a newborn baby being abducted. Criminal acts could be theft of patients' belongings, money from any commercial outlet, equipment or drugs. (Aldridge, 2005). Traditionally the public has had easy access to many parts of a hospital but with the increasing risks of litigation related to claims of negligence the issue of identification needs to be seriously addressed.

Tracking

In an emergency situation speed is vital when attempting to locate the required staff, equipment and the patient at risk. There are various tracking systems available that provide real-time, wireless tracking of patients, medical equipment and staff. Some systems embed the identifier in a badge whilst others use wrist bands or adhesive labels. The systems also help the hospitals "to efficiently match resources as patient flow fluctuates and to further analyse department utilisation" (PCTS, 2006).

The SARS outbreak in Asia was the catalyst for a tracking system in the Accident and Emergency Departments of a Singapore hospital. The system tracks patients, staff and visitors using a card containing an RFID chip and sensors installed in the ceilings. It stores information for 21 days, so that in the event of an outbreak all individuals with whom an infected person has been in contact can be traced. It is expected that the system will be adopted by other hospitals in Singapore. (EPIC, nd).

The paperless office concept is being adopted as an effective method of managing treatment and patients with the introduction of systems that feature "electronic chemotherapy prescribing, safety tools and pharmacy dispensing all linked up to a patient record, as well as the ability to collect and analyse research data through clinical trial participation." (E-health Insider, 2004). Also, some emergency and surgical departments in UK and US hospitals have large plasma screens to monitor bed status for more efficient allocation and to provide relatives with an up to date patient status during surgical procedures.

Other hospital applications include an RFID system that tags "patients at risk of falling, wandering off or otherwise endangering themselves" (Bacheldor, 2006). Other uses of RFID in a hospital environment are asset tracking of equipment, plus tracking of samples and drugs.

Storing information

The amount of information being gathered about patients and staff in particular is increasing with the use of electronic surveillance systems. There is already a large amount of electronic information stored about patients in electronic health record systems which governments are recommending as the method of data storage rather than paper-based record systems (Australian Privacy Foundation, 2006). Other information that might previously have been stored with the physical record such as x-rays, pathology reports, etc., are now more likely to be digital and therefore can be linked directly to each patient's electronic health record. Currently, surveillance information is not linked to the patient health records. However, in future that may change as the security requirements become a more important priority due to the perceived increase in threat levels. This change will affect staff, contractors and visitors as well as patients as the increased surveillance information has the potential to be amalgamated and analysed in order to provide additional intelligence.

ELECTRONIC SURVEILLANCE SYSTEMS

There are a number of electronic surveillance methods in use and these are becoming more common in a hospital environment. The main ones are CCTV, access control cards, smart cards and RFID.

CCTV

CCTV is not a new form of surveillance. However, the latest form of CCTV is digital rather than analogue and can be linked to other systems such as the as access control systems (Aldridge, 2005). The placement of CCTV is important and will normally include all areas within the hospital where risk is high, such as birthing centres, nurseries, ATM machines, cashiers, pharmacies, egress points and public car parks.

Access Control/ Smart Card

Access Control systems are used to restrict access to certain areas of the hospital based on a person's role (Hu, Ferraiolo & Kuhn, 2006). The access cards used may or may not be used for identification as well as access control, but increasingly this function is included. The card will often be a smart card of some sort with the photo id printed form a digital image held on the system. The card will normally display the person's name, department and possibly their job title. The card is required to allow access to restricted areas of the hospital. The system stores details of the person who passed through each access point and at what time. Smart cards systems may be used for other purposes also, such as a library card or an electronic purse for use within the hospital.

RFID

Radio Frequency ID is not new, but the technology that it uses has improved over the past few years. There are now active as well as passive tags that use various frequency ranges which work over short, medium or long distance depending on the frequency used. Active tags contain an independent power source that allows the data to be updated whilst the tag is in use. A passive tag has no independent power source but it is intended to be a unique identifier and therefore can uniquely identify whatever it is attached to, which may be a blood sample, a portable x-ray machine, or a patient's wristband. The tags are read by readers that are embedded in ceilings, walls or door frames. (Olenwa & Ciampa,,2007, chapter 11).

There are also firms offering implanted RFID devices for various applications such as patients with chronic conditions, particularly if the condition causes them to be non-responsive during an attack or episode of the illness. There are a quite a number of people, including physicians, who have implanted RFID devices into various parts of their body as an experiment to measure the effects and effectiveness of the device (Schuman, 2005).

Vendors of RFID solutions are offering similar features as those found in smart card systems, such as "an e-purse for cashless transactions" (Dassnagar, nd) and for improved tracking they can add GPS technology.

RISKS TO INFORMATION PRIVACY AND SECURITY

In an on-line world the risks to information are many. They can come from staff, patients, relatives, or unrelated persons who may try to alter, damage or disclose information to affect its integrity or confidentiality. This may be due to a physical action of some sort or as a result of a digital attack. For example, information held digitally is at risk of disclosure if an unauthorised person is able to read confidential details off a computer monitor; equally at risk is electronic information that is inadequately protected enabling someone to copy, modify or delete confidential information. In both these examples it is more than likely that the disclosure will not be detected. In the case of modification or deletion these may be detected by audit programs or eagle-eyed staff members, but detection is not guaranteed and the result could cause harm or death to a patient. The impact on the hospital could be severe due to the resultant litigation and bad publicity (Aldridge, 2005).

Ownership of information

There are guidelines for the protection of medical records and related patient information. However, these may not cover information gathered via surveillance devices. In a hospital with CCTV, access control and RFID devices each system may be administered and monitored by different groups. Security staff may administer the CCTV and the access control systems whilst the RFID system is administered by a different group. Often these functions may be outsourced to a private company which may maintain the information on site or they may store and analyse it off-site. However, the information gathered could all be stored in one area, even though it will be administered by different groups. This increases the risk that the information could be subject to unauthorised data matching and analysis.

Implications for Privacy

The issue of data matching is significant in the health area at a time when law enforcement and government agencies are being given increased powers that can impact on the expectation of privacy.

The privacy laws (Privacy Act 1988 (Cth) s. 95A) allow information to be used for a purpose other than that for which it was collected in certain circumstances which include:

> If the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
>
> or
>
> use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Interpretation of these will depend on the person making the decision, the circumstances at the time and any other pressures that are being exerted on that person.

Implications for Security

According to leading healthcare lawyer Kirk J .Nahra "A security breach that discloses substantial health information could lead to other kinds of privacy harm (embarrassment, reputation injury, etc.)" (Nahra, 2005). Individuals may gain information that allows them to compromise, blackmail or affect the reputation of another person by providing them with medical, personal and financial details that could be used against them. Therefore, information security practices need to be examined in order to avoid breaches that could lead to litigation.

ISSUES THAT NEED TO BE ADDRESSED

There are a number of issues that need to be addressed to protect a hospital's information. These include the standard information security measures that would be expected to be in place in an organisation of this size and type. However, due to the nature of the organisation special interest should be paid to privacy issues.

Privacy Policy Compliance

Hospitals need to ensure that the principles in the Privacy Policy are being adhered to by all staff, contractors and organisations who handle the hospital's information. This is particularly important when the information is being processed and stored off-site. Standards for protection of this information need to be included in contracts for both staff and contracted organisations in order to avoid breaches of the policy. Currently, in Australia there are standards covering the management, operation and application of CCTV. The "Standard aims to provide good practice to assist owners in obtaining reliable information that may be used as evidence. Compliance with this Standard is strongly recommended, particularly where CCTV systems include an element of observation of the public." (Standards Australia, 2006). Currently in draft form, the CCTV Standard Part 4: Remote video monitoring, specifically states that "As a code of practice, this Australian Standard should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading." (Standards Australia, 200X). Consequently, it is essential that hospitals take steps to ensure that the operators and managers of their CCTV comply with the Australian standards.

Awareness

Breaches of policy are more often due to lack of awareness or understanding of the issues, or staff working under undue stress, than to overt behaviour (Patel, 2002, p.222). Education and training programmes should be implemented to ensure that lack of awareness is not a cause of policy breaches. Policies for acceptable use of information and information systems need to be developed, implemented and policed.

Legislation and Standards

Currently, there are a number of pieces of legislation and sets of standards pertaining to this area at both State and Federal level. These include the Privacy Act (Privacy Act 1988 (Cth) s. 95A) and the Australian Standards for CCTV (Standards Australia, 2006) which state that:

> Because there is separate Federal, State and Territory Privacy and Surveillance Legislation in Australia it is the owners' and their advisers' responsibility to make themselves fully aware of the Privacy and Surveillance Legislation that applies to their State or Territory in relation to CCTV systems.

The expectation of the standards is that owners and administrators of these systems will abide by the standards and operate in a manner that reflects best practice.

CONCLUSION

A large amount of information is collected and stored in the hospital environment. Some of this information is core to treatment and is held on the patient's medical record. Other patient information is held in various hospital information systems for administration, identification and tracking purposes. Surveillance information from CCTV is held separately, though not necessarily by the hospital. At present this information is not used for data matching purposes except where that is core to the purpose of the information collection. However, the potential to do so exists and with the current government predilection for tightening security there is the attraction of constructing an electronic footprint for each individual.

RFID use is increasing in the hospital sector and this is being linked with the patient medical record as it is becoming core to treatment in some hospitals. The indications are that this will become normal practice which means that surveillance information from RFID systems will be linked much more closely to a patient's medical record. The risks to information from such collection sources can affect ownership and patient privacy, with the issues of policy compliance, legislation and user awareness still to be addressed.

The benefits of electronic surveillance to patient health are manifold, but it is vital that the privacy implications for individuals are not overlooked by the motivation to achieve security for the whole community.

REFERENCES

Aldridge, J. (2005). Hospital Security: the past, the present, and the future. *SecurityInfoWatch.com.* Retrieved 28 October, 2006 from http://www.securityinfowatch.com/article/article.jsp?siteSection=357&id=5719

Australian Law Reform Commission/Australian Health Ethics Committee, (2002). *Joint Inquiry into the Protection of Human Genetic Information.* Submission from the Federal privacy Commissioner. Retrieved 28 October from http://www.privacy.gov.au/publications/genesub.pdf

Australian Privacy Foundation (2005). Re: Review of the Regulation of Access to Communications under the Telecommunications (Interception) Act 1979. Submission by the Australian Privacy Foundation. Retrieved 16 November 2006 from http://www.privacy.org.au/Papers/SubmTelecomIntercept050520.pdf

Australian Privacy Foundation (2005). Electronic Health Records. Retrieved 16 November 2006 from http://www.privacy.org.au/Campaigns/E_Health_Record/

Bacheldor, B. (2006). RFID System Helps Houston VA Hospital Maintain Patient Safety. *RFiD Journal.* Retrieved 16 November 2006 from http://www.rfidjournal.com/article/articleview/2732/

Bart, C.K. & Hupfer, M.(2004). Mission statements in Canadian Hospitals, *Journal of Health Organization and Management.* Vol 18 No 2, 92-110.

Collins, J. (2004). RFID Remedy for Medical Errors. *RFiD Journal.* Retrieved 16 November 2006. http://www.rfidjournal.com/article/view/961

Collins, J. (2006). U.K. Surgery Ward Tags Patients, Tracks operations. *RFiD Journal.* Retrieved 16 November 2006. http://www.rfidjournal.com/article/articleview/2561/1/1/

Crompton, M. (2001). *Guidelines on Privacy in the Private Health Sector*. Retrieved 31 October 2006 from http://www.privacy.gov.au/publications/hg_01.pdf

Dassnagar. *RFID in hospitals.* Retrieved 31 October 2006 from http://www.dassnagar.com/Software/AMgm/RF_products/it_RF_hospitals.htm

E-Health Insider (2004). *Norfolk hospital gets electronic cancer care system.* Retrieved 31 October 2006 from http://www.e-health-insider.com/news/item.cfm?ID=821

EPIC. *Radio Frequency Identification (RFID) Systems: Tracking patients and personnel.* Retrieved 31 October 2006 from http://www.epic.org/privacy/rfid/

Evans, N.D. (2006). Where is RFID's ROI in health Care? *RFiD Journal.* Retrieved 16 November 2006. http://www.rfidjournal.com/article/articleview/2124/1/82/

Hu, VC, Ferrraiolo, DF & Kuhn, DR (2006). *Assessment of Access Control Systems.* National Institute of Standards and Technology, Technology Administration, US Department of Commerce.

Nahra, K.J. (2005). Federal Security Breach Legislation Progresses (but slowly). *Privacy in Focus.* Retrieved 16 November 2006 from http://www.wrf.com/publication_newsletters.cfm?id=10&publication_ID=12393

OCR HIPAA Privacy (2003). *Marketing.* Retrieved 16 November 2006. http://www.hhs.gov/ocr/hipaa/guidelines/marketing.pdf

PCTS (2006). Christiana Care Installs Patient Care Technology Systems' Automatic Tracking Software in Second Facility**.** Retrieved 31 October 2006 from http://www.pcts.com/News/Press/pr_Wilmington_Passive_Tracking_090705.asp

Olenewa, J. & Ciampa, M. (2007). *Wireless Guide to Wireless Communications.* Boston, Massachusetts: Thompson Course Technology.

OSH Act (1970) (US) section 5A. Retrieved 31 October 2006 from http://www.osha.gov/SLTC/healthcarefacilities/index.html

Patel, A. (2002). IT Security Training in the Healthcare Environment. In E.B.Barber, B.Blobel, K.Louwerse & B.Barber *Eds.), *Security Standards in Healthcare Information Systems.* IOS Press.

Privacy Act (1988) Act No. 119 of 1998 as amended, taking into account amendments up to Act No. 99 of 2006, section 95A *Guidelines for National Privacy Principles about Health information.*

Schuman, E. (2005). CIO Tests Embedded RFID Chip. *eWeek.com.* Retrieved 31 October 2006 from http://www.eweek.com/article2/0,1895,1756577,00.asp

Standards Australia (2006). *Closed Circuit Television (CCTV) AS 4806.1-2006. Management and operation.* Standards Australia, Sydney, NSW.

Standards Australia (200X). *Closed Circuit Television (CCTV)* Draft for Public Comment Australian Standard. To be *AS 4806.4-200X. Remote Video Monitoring – code of Practice.* Standards Australia, Sydney, NSW.

The National Patient Safety Agency (2004). *Right patient – right care.* London:NHS.

The Office of the Privacy Commissioner (2006). *Annual Report 2005-06, Chaper 1 Respecting Privacy.* Retrieved 16 November 2006. http://www.privacy.gov.au/publications/06annrep/c1.html#exposure

COPYRIGHT