

Confidentiality and Privacy with Health ICT

An introduction paper by:

Dr Peter R Croll

Chair of HIPS, HISA Privacy in Health Forum

Director, Health Informatics Society of Australia (HISA Ltd.)

Owner, Better Life ICT (www.blict.com)

Introduction

In matters of health we can expect some degree of confidentiality when dealing with a healthcare provider. How much will depend on the circumstances and who we are dealing with at that time. Let us consider two extremes of the spectrum when dealing with issues of confidentiality.

On the one extreme, where someone was discussing their mental state with a psychologist, we would expect the highest level of confidentiality to apply. The patient has taken the psychologist in their confidence and expects whatever has been said to remain with them. The psychologist may wish to discuss aspects with his colleagues to gain a better insight to the case. The patient would reasonably assume that their psychologist would not personally identify them in such discussions unless they had given their specific permission to do so.

On the opposite extreme someone might be telling a person they don't know particularly well that they often suffer from migraines. They would not subsequently be too surprised if this person then mentioned this to others, especially if this occurred in a public place like a party or social gathering.

These extreme examples highlight the two key issues associated with confidentiality:

Who are you telling, and;

What are you telling them?

There are assumptions made regarding confidentiality that are associated with the type of person and how sensitive the information is that you are revealing to them. A person's type might be determined by their profession which in turn can influence the sensitivity issues.

With the medical profession the need to establish the highest ethical standards has been evident for over 2000 years. This can be traced back to the 'Hippocratic Oath' believed to originate from around the 4th Century BC most probably from Hippocrates, sometimes known as the father of medicine. It has been the tradition for physicians to take up the oath, although this is no longer obligatory, as a rite of passage for medical practitioners. Translated from the original Greek the excerpt in the Oath relating to confidentiality reads: "Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." [Harvard 1910]. Physicians would encapsulate these values by ensuring that discussion about an individual's conditions be confined within a practice or department for the primary purpose of helping the patient concerned. Secondary use of information that can be highly beneficial to the advancement of medical knowledge. In this case it would normally practice to avoid identifying the individual concerned unless they had consented.

The more recent advancement of digital technology and e-health is providing a revolution in both medical know-how and healthcare provision. But with this advance the traditional boundaries are being breached. The concept of confining information in written form to a physical location, such as a surgery, is gradually disappearing. The remote and high speed access that today's digital technology brings presents new challenges and not only with healthcare providers but for governments, the ICT industries, lawyers and individuals alike.

Until the advent of the electronic computer and high speed communications confidentiality has been much easier to control. With spoken and written manual records it has been much easier to direct one's sensitive information to the right people. Judgements can be made about whom you trust and how much you tell them. This can limit the amount of sensitive information that is available in any one location. For example, even if you find out that with their paper records your general practitioner or local hospital is somewhat lax with confidentiality you are less likely to be worried about this being linked to your psychiatric reports. With a centralised electronic record system there may be more cause for concern. Although this may not be the case in practice, the concern is that you have to trust systems that you may not be familiar with and people that are unknown to you. The reliance on third party support is widely adopted with today's IT systems. With the many media reports of privacy violations with electronic based information it is difficult to know who to trust and how to judge them. IT privacy and security issues are addressed in more detail later in this paper since they are an essential component in the trust paradigm. If you don't trust the systems being employed you cannot be sure that confidentiality of your sensitive information will be adequately handled.

The following diagram shows the basic relationship between Confidentiality, Trust and Privacy. This has been introduced to help simplify your understanding of these important aspects. Much of the text that can be read on this subject area attempt to define each term. Unfortunately there is not much consistency in these definitions. In addition, although many definitions are factually correct, they can be hard to decipher as to their meaning in any practical sense with the handling of personal information. Hence the following diagram is used to identify the key concerns. Later in this paper, the relationships are developed further to introduce security and safety.

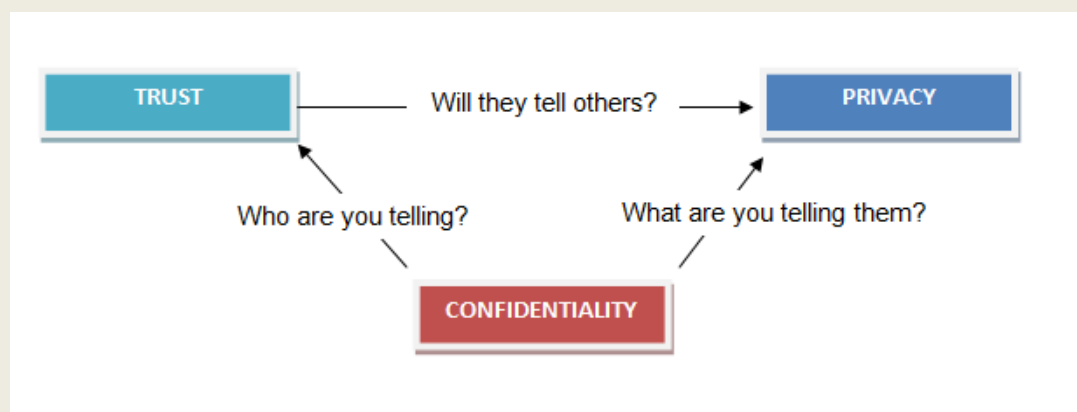


Figure 1. Confidentiality, Trust and Privacy mapping.

Before we look at privacy and security, let us consider why it is now more challenging to be sure about confidentiality with IT systems:

1. The key issue of 'who are you telling' has been extended beyond just your medical practitioner to include others who have access rights (including non-medical technical staff);
2. The key issue of 'what you are telling them' does not necessarily get handled any differently inside the computer system (except in the less common cases where different degrees of data sensitivity measures have been built in);
3. You have to place trust with systems that have third party support (including maintenance and backup);
4. IT security is a challenging topic for all concerned and it is not necessarily well understood by the medical professionals who are responsible for good governance measures to minimise the risks;
5. The media regularly reports on privacy violations with computer systems and it is difficult to judge what measures have been employed to protect your information from similar occurrences.

The key learning objective with this paper is to appreciate what the critical criteria are for providing confidential IT systems used for health and to understand the best approach for achieving a trusted solution.

Trust with Health Information

The previous section looked at Confidentiality in the context of health information. We identified that there is a direct relationship with Trust. For the purpose of health information we have focussed here on the human aspects of Trust. There is a lot of literature that now talks about 'Trusted Systems' in the context of computer systems that demonstrate high reliability, integrity and security measures. These are important technical aspects and will be addressed later in this paper. There is a good reason to separate out the human from the technical aspects because traditionally they are measured and handled in different ways. Attempting to use the same analysis techniques can result in widely differing results due to the types and range of users we find across the healthcare spectrum. When non-technical people are asked to gage their trust they generally give more weighting on perception rather than facts since with IT systems, topics like reliability, security and integrity are all complex and technically demanding to comprehend. Technical people can themselves be frustrated by these perceptions, as is evident in the electronic banking sector, but there is growing evidence they are now adopting measures to accommodate these perceived fears [Croll 2006b].

The relationship developed between Confidentiality and Trust was "Who are you Telling". Note that the emphasis here is on 'Who' not 'What'. For the average member of the public the Trust they place on a computer system will depend mostly on who owns and operates it. People generally trust their Doctors and other qualified medical staff. They extend this trust to the services and equipment they employ in the doctor's practice. Only in the infrequent cases where the patient is knowledgeable about the computer systems being used and the manner that the medical staff use them can they make any informed judgement. In the absence of direct health IT knowledge, or any adverse prior experience of these IT systems failing, they rely heavily on their perception. Hence, from the view of the general public, Trust relates more with the people they deal with. This extends beyond the public since many medical staff are often just as poorly informed with the technical side of computing. Finding the truth requires this in-depth technical knowledge. Unlike other safety conscious industries, such as aviation, there is no mandatory investigation or central reporting facility when computers fail. It is therefore difficult to locate a trusted body of knowledge that can provide objective answers to the reliability and integrity of a given IT system.

Privacy with Health Information

Everyone is in agreement that Privacy is a high priority when dealing with Health Information. The response on how to deal with Privacy does get confused with the measures needed for IT Security. How they differ is explained through examples given below. Attaining absolute privacy is not particularly conducive with healthcare. If we adopt the definition of privacy as "*a person's right to be left alone*" then it would be obvious that they could not be left completely alone as healthcare requires some interaction with the person and knowledge of their condition.

The expression 'striking the right balance' is often used to describe how issues of privacy need to be weighed against benefit for the patients. This is particularly evident when health data is used for research purposes. The balance being struck here is the risk of privacy violation against the outcomes for the good of the public. Looking at health data, even if the patients identifying information has been removed, this runs the risk that someone might be able to determine to whom that data belongs. This is particularly true when either the individual in question is known by the researcher or the individual has either unique or an unusual set of conditions making them easier to trace. So when data is used or presented there is always some privacy risk. Measures can be put in place to minimise these risks are discussed later in this paper.

The public good aspect refers to what positive outcomes can be derived from allowing health data to be used for research purposes. It may provide new valuable knowledge in population health studies or help identify an outbreak of an infectious disease. Too rigid a privacy policy will limit the effectiveness of health knowledge discovery while too loose a policy may result in an unacceptable number of privacy violations.

Finding the right balance for research can be ascertained by an ethics committee who will judge the risks and benefits. From an individual's perspective it is less clear how this is achieved. Many privacy advocates stress the need for individuals to have 'control' over their personal data. The law of most countries that have health privacy legislation usually allow for individuals to have the 'right' to determine the privacy of their data. Having the right and having control are not the same thing. Since, with IT systems, the patients rarely enter the data or own the computer systems. They have to give up their control to the medical staff involved. To further compound this, medical staff usually depend on third party support to determine the degree of control they actually have. That is, control is determined by the applications, the operating systems, the database systems, the policies and procedures of the organisation and IT or technical staff.

This emphasises the relationship between Trust (of the individuals involved) and Privacy as shown in diagram 1 as: "Will they tell others?" We have to trust that the individuals involved provide a supportive system that will minimise the risk of inappropriately disclosing personal information. The supportive system stretches well beyond the IT system and has to include implementation of those policies and procedures that make up good governance of your personal information. For example, when admitted to a hospital or medical clinic where you are asked to sign a consent form that included statements about who can see your personal data and for what purpose. Privacy policies and consent forms are varied in healthcare. Some act more to protect the individual others to protect the organisation from legal recourse. It is usually the latter that dominates.

How does Privacy differ from Security?

To appreciate the difference between privacy and security consider an exhibition that is displaying valuable antiques. The display cabinets can be made of reinforced glass and well secured. The contents are intentionally visible for all to see but kept locked to prevent anyone from stealing them. Now with an IT system such stealing might involve using a removable storage device such as a memory stick or even an MPEG player to remove data. This could also be achieved remotely via the Internet or other network connections. A range of security measures can be employed to prevent unauthorised copying of information, e.g., firewalls, smartcards or one of a number of password protected access control mechanisms [Liu *et al* 2007]. A privacy violation might not involve copying and stealing data but simply viewing it as in the case of the exhibition display cabinets. To view private information either on a screen or because your account access rights permit it may well be improper. This is more likely to occur internally within an organisation due to the IT security measures put in place but need not be the case if the system is configured to allow remote viewing. One of the main problems facing organisations is determining what constitutes an unauthorised person viewing a record and how to handle this in a pragmatic manner. Because of the way contemporary systems are configured some people have wide ranging access rights. For example, in Australia we have seen this problem emerge with the Tax Office and the social service department Centrelink [ABC 2006]. From a medical view point, personal data should only be viewable on a 'need-to-know' basis. That is, the individuals concerned should be part of a case file, or they have given consent permission to look at their information, or their life is in danger, or access has legal authority.

Consent is a complex and often emotive issue. It is not always clear-cut that permission may have been granted for general access within a healthcare organisation and, furthermore, each organisation and even divisions within the same health authority often develop and use their own consent forms. The legal standing of these forms again is often unclear and one of the reasons why, for example, the Health Informatics Society of Australia (HISA) has in a submission to the Australian Law Reform Commission [ALRC 2007] strongly recommended changes.

When it comes to health information you cannot talk about security without reference to privacy. Health information relates to individuals, either staff or patients and any security measures must try to protect the privacy of that individual. Also, it is not easy to segregate these issues within any electronic implementation since access control, cryptography and authentication are essential security mechanisms that also provide degrees of privacy protection.

The simplest way to differentiate these issues is to consider health Security as the mechanisms used to keep unauthorised people out and Privacy as the way that authorised people can only see information on a 'need-to-know' basis. The two issues for health security access mechanisms therefore are:

Restrict to only those authorised and trustworthy, and;

Restrict to only those that need to know.

The following diagram shows these relationships with Trust and Privacy:

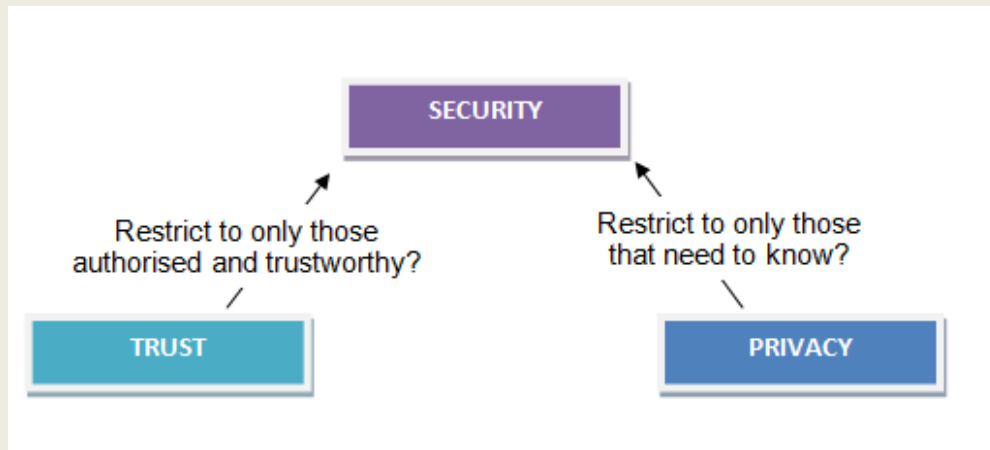


Figure 2. Security, Trust and Privacy mapping.

Access Control Mechanisms

Computer systems can employ a number of control mechanisms to provide privacy and security for personal and sensitive data. These originated as a means of limiting the damage that the inexperienced user might make on a system. That is access to certain files and programs and whether they could add, delete or modify them could be controlled to some degree at the discretion of the administrator (also known as the Superuser). This basic mechanism still forms part of the majority of today's computer operating systems and is referred to as a DAC (Discretionary Access Control) mechanism. Other more stringent methods have been employed such as MAC (Mandatory Access Control) mechanism that use specialised access control policies to mandate who can see and run all the objects that make up a system. Within the programs themselves RBAC (Role Based Access Control) mechanisms have been employed that specify who can do what based on the job function within an organisation. Note that this program protection mechanism is referred to as an 'application level' protection as opposed to 'systems level' protection. A systems level protection is much safer as any application level protection can be more easily bypassed by knowledgeable users or hackers. Whatever mechanism is employed no mechanism is 100% safe from misuse and the risks need to be determined and weighed up against the cost of protection. Furthermore, as security mechanisms are introduced then other factors such as ease of access and usability can be detrimentally affected.

Internet and Network Protection

The biggest challenge is to provide protection mechanisms that prevent unauthorised access from the network connections, particularly the global Internet. Allowing remote access can be highly beneficial to an

organisation but that can allow for unauthorised anonymous users to hack their way into the system. The careful governance and auditing of accounts, use of strong passwords, restriction to specific machines and encryption of data using secret keys will reduce these risks significantly. With the Internet there are many occasions when this is not suited to the business model. Ingenious mechanisms such as PKI have been developed that allow for a compromise yet provide a fair degree of security. PKI stands for Public Key Infrastructure which is a method of using publicly available access keys together with trusted third party authorities to allow medium level security remote access for the general public across the Internet. Public key certificates and the associated asymmetric cryptography is sophisticated and complex and hence often misunderstood. It is therefore frequently and inappropriately suggested as the best solution for many problems in healthcare Internet security. It has a role to play like the many solutions that are commercially available but will not necessarily provide the degree of security and privacy that sensitive health information requires. The failing is not necessarily the mechanisms employed but how they are governed and more importantly how well protected the personal computers are that connect to the network. Ensuring good Internet protection will remain a challenging problem for the foreseeable future.

Safety and Quality

Since the publication of the alarming rates of safety in public hospitals the drive towards safety and quality has been intensified. The report 'To Err is Human...' showed that error rates and fatalities far exceeded any other industry including the automotive one [Kohn 2000]. Computerised systems were regarded as an essential tool to reduce errors, particularly in areas of medication management. For example, doctor's handwriting has always been notoriously difficult to read and the use of printed pharmaceutical prescriptions together with the ability to do some automatic checks on dosage, interactions etc. should dramatically reduce some of these errors. Compared with pen and paper, computer systems are a more complex technology and can themselves fail in unsuspected and subtle ways. Any computer mechanism that is introduced to reduce harm should be assessed to see if it can itself cause harm. This is a non-trivial task as the level of understanding required to do a safety assessment on computer technology is very challenging. Awareness of these safety issues is very important especially when people's lives are at risk.

A safe system should be the central basis from which electronic healthcare systems are derived. As discussed above, security can have a detrimental effect on other quality factors such as usability and ease of access. These in turn can have a detriment effect on safety as there are many interdependencies in a given software design [Croll 2007]. In this paper we are focussing on Privacy, Security and Trust. For Privacy the concern is what harm can be caused by inappropriate access to your personal information. For security the concern is the harm that any modified or corrupted information (i.e. the data integrity) may have on safety. For Trust the concern is if the people you have entrusted your health with will do what is required to protect your information. These key issues can be stated as:

Can what they know harm you;

Can poor integrity harm you, and;

Will the people you trust protect you?

Figure 3 completes the picture in terms of Privacy, Security, Confidentiality and Trust by placing Safety as the central issue.

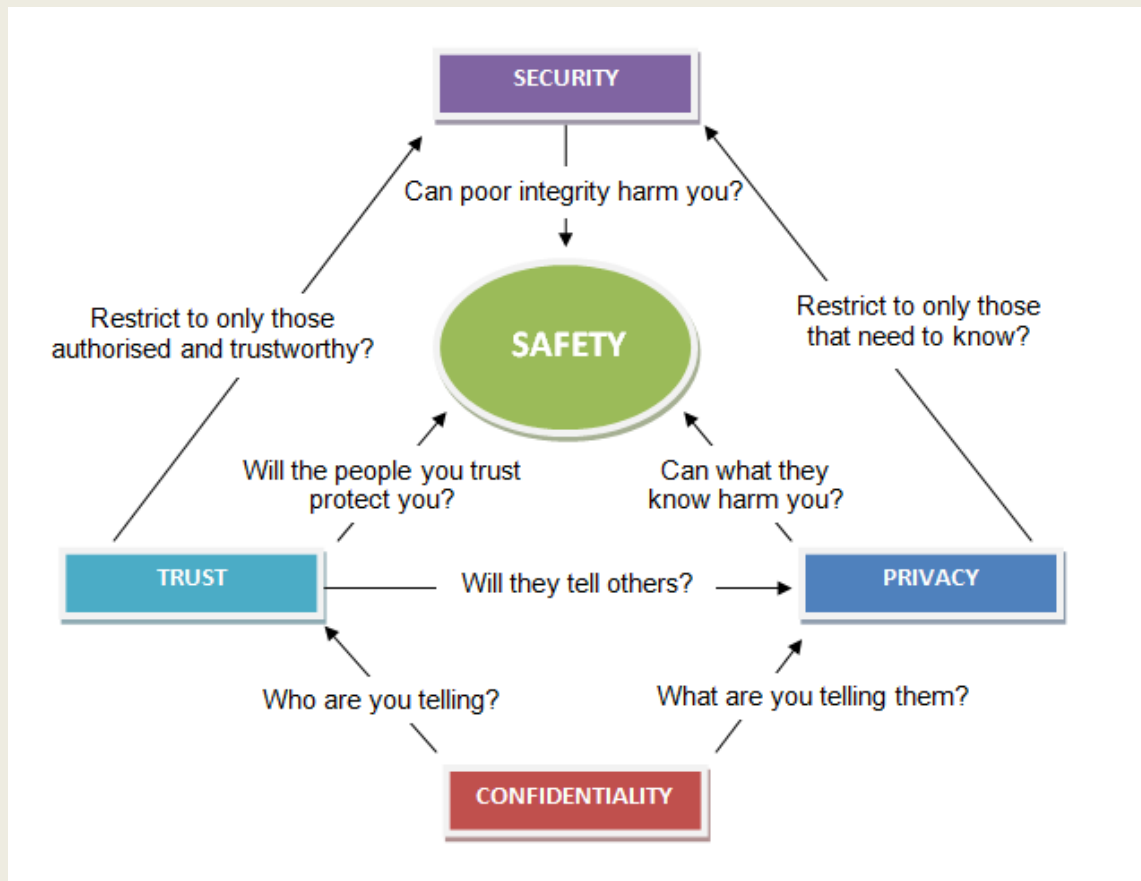


Figure 3. Safety at the centre of the Privacy, Confidentiality, Security and Trust mapping.

Conclusions

Confidentiality is a fundamental requirement with health services. Its wider application with today's electronic computer systems requires adequate privacy policies and trust in the systems deployed. This is more challenging due to the common use of third party vendors to supply computer systems and the separation of control away from the medical practitioner who has built up your trust. Privacy and Security are often misunderstood terms that get used interchangeably. The computer implementations only add to this confusion by employing mechanisms that handle both through the same technology. The model produced in this paper clearly identifies the complementary roles each has to perform for health information. Security mechanisms have been outlined that can provide a wide range of protection. These all come at a cost, not only financially but in terms of restricting other quality attributes such as usability and ease of access. Any quality health service should put the patient first and have the highest standards in terms of 'safety and quality'. It has been demonstrated that safety can be made the central attribute in a trustworthy system and the key issues that relate each property can be identified in an unambiguous manner.

References:

- [ABC 2006] "Centrelink staff sacked for privacy breaches", news report ABC online, Wed, Aug 23, 2006.
- [ALRC 2007] "Review of the Australian Privacy Law", Discussion paper 72, Australian Law Reform Commission (www.alrc.gov.au), Sept 2007.
- [AS17799 2006] AS17799:2006 – Information Technology Security Techniques – Code of practice for information security management, Standards Australia.
- [Croll 2006a] PR Croll & J Croll, Privacy Compliance – Managing the Risks when Integrating Health Data, Health Informatics Conference Sydney, Aug. HIC 2006.
- [Croll 2006b] Croll, PR.& Morarji, H. (2006) Perceived Risk: Human Factors Affecting ICT of Critical Infrastructure. Proc. The Social Implications of Inf. Security Measures on Citizens and Business, pp. 213-222
- [Croll 2007] PR Croll and J Croll, Investigating risk exposure in e-health systems . International Journal of Medical Informatics , Volume 76 , Issue 5 - 6 , Pages 460 - 465
- [Croll 2008] PR Croll, Special Issue: Health Information Privacy and Security, electronic Journal of Health Informatics [ww.eJHI.net](http://www.eJHI.net), Vol 3, No 1 (2008).
- [Harvard 1910] "Harvard Classics, Volume 38" Copyright 1910 by P.F. Collier and Son.
- [Jones 2007] Safeguarding personal information, LEGISLATIVE COUNSEL'S DIGEST AB 1298, Bill introduced by Assembly Member Jones, State Legislation California, 2007.
- [Kohn 200] Kohn LT, Corrigan JM, Donaldson M, eds. To Err Is Human: Building a Safer Health System. Committee on Quality of Health Care in America. Institute of Medicine; 2000.
- [Liu 2008] V. Liu, L. May, W. Caelli, P. Croll, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis, electronic Journal of Health Informatics, 2008; 3(1): e3.
- [Lui 2007] Vicky Liu, L May, W Caelli, P Croll, A Sustainable Approach to Security and Privacy in Health Information Systems, 18th Aus Conf. on Information Systems (ACIS'07), Dec 2007 , pp 225- 265.
- [Magnusson 2004] Roger Magnusson, 'The changing legal and conceptual shape of health care privacy' (2004) 32 Journal of Law, Medicine & Ethics 680-691.
- [PIA 2006] Privacy Impact Assessment, Australian Government, Office of the Privacy Commissioner (www.privacy.gov.au), Aug 2006.