Privacy, Security and Ethics

Security can be a complete show-stopper - get it wrong once and you most probably won't get a second chance, at least not for a considerable time. Expectations, law, ethics, technology, politics ... they all tie together into a continuously moving complex. Let us help you through the maze.

We've successfully addressed these issues for clients in different parts of the globe. We have issues and discussion papers, technology-based and non-technical elements to our comprehensive solutions outlines. It's an intensive area, but we have developed a series of workshops to help you understand the issues and concepts.

Why not read and print this overview page, and then
contact us by email today (consulting@hic-ltd.com) outlining your particular interests or concerns - or
- to enquire specifically about our *'International Healthcare Workshops'* programs.

We'll respond and if you need them, we can send you copies of some key *White Papers* and / or *Articles* of particular relevance (ie discussions on our NZ, Australia and European experiences). We would be delighted to discuss key issues and topics related to your plans and developments.

---

1. What is security? Privacy? Confidentiality?

Security, in computing terms, is generally considered in terms of the triad: **availability, integrity and confidentiality**. **Availability** relates to the expectation that authorised access to information will be freely available at all times to authorised persons; **integrity** relates to the expectation that a system will do what a reasonable person would expect and nothing else; and **confidentiality** relates to the expectation that information will be stored in a way that prevents unauthorised access or disclosure. **Privacy** is the corollary of confidentiality – the expectation on the part of the subject that their personal information will be kept secret and confidential by the holder of it.

Most jurisdictions have legislation that pertains to these issues, but, unfortunately, it is very patchy and variable. Privacy of information is general recognised as the third of the personal privacies, after privacy of the person (eg against assault) and privacy of property (eg against theft). However whilst the former privacies are recognised under most legal systems, privacy of information may not. Nevertheless health professionals have been ethically committed to it for thousands of years. The Hippocratic Oath (the ethical gold-standard for doctors) has a section that reads:
'Whatever in connection with my professional practice, 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.'

Interference with computer systems is a growing 'sport', and hacking into a system is a challenge that seems to be of particular interest. However most breaches of security (>90%) at the present time are perpetrated by individuals who are authorised system users who have exceeded their authority. Detection of such abuses may not be easy, especially with older systems, and punishment of offenders may be impossible, or inadequate in the context of the damage they may have done.

Back to Top

---

2. What is so important about these in healthcare applications?

Healthcare information is often of a very intimate nature – revealing aspects of a person that they may have no wish to share with anyone except in the content of receiving appropriate professional care. Electronically stored information may become lost, corrupted, altered or improperly disclosed. Any one of these events could cause distress to patient and/or provider. Although common also in paper records, these problems are especially acute in computerised systems where a major aspect of the design philosophy is to ensure ready accessibility to larger numbers of authorised users, and to accumulate progressively more and more information. The number of potential users of a 'system' is limited only by the extent of the networks to which the information store is knowingly or unknowingly connected – often literally the world and therefore also to global 'hackers'.

Back to Top

---

3. Where do current practices go wrong? Is this just a computer problem?

Current practices in relation to security issues are for the most part inadequate. Often we

do not recognise how sensitive apparently innocuous items of data may be to the parties concerned, and few people are aware of just how insecure data can be, whether stored on a computer or as hard copy. There is a certain 'paternalism' that has pervaded healthcare, along the lines that 'your information is safe with us – but research shows that this is simply not true. Few healthcare organisations, large or small, have developed proper security policies and plans and ensured that these are communicated to staff and patients: many have not even seriously considered the issues or risks. Hard copy records have in the past been perversely secure for two reasons: there has been only one physical copy, often not readily located; and it has been so poorly organised and illegible that abstracting information from it has been difficult. Computers have eliminated these obstacles.

Computerised and hard copy information differ in two fundamental ways. One difference relates to perception: hard copy information is something we are all familiar with, and feel that we 'understand'. By contrast, information that is stored in electronic form is 'mysterious', and therefore a source of anxiety. Understandably, therefore, the public is more concerned about the security of electronic records, especially not knowing where it is stored or who controls it. Nebulous assurances regarding security and storage technologies simply add to the worry. The various well-publicised failures of computerised systems have served only to contribute to this unease.

The second striking difference is that electronically stored data can be manipulated in ways that are impossible with hard copy. For example searching, sorting into categories, matching and linking one set of data with another and even with other databases, is relatively easy to do with electronic records, but difficult with hard copy. Further, these functions can be performed remotely without the user ever being in physical contact with the stored materials.

Back to Top

---

4. Where do we start?

There is a lot to do. But the key issue is to be aware of the issues and continually to test the proposed solution in the context of these issue.

4.1 Politics and ethical considerations

Without doubt the biggest show-stopper in terms of large scale healthcare systems proposals is a suggestion that security is inadequate: professionals and the community are increasingly vocal in their opposition to systems with unqualified security concerns.

The ethical situation is clear: in terms of availability, integrity and confidentiality the expectations of the providers of both care and information management services are self-evident. As far as availability and integrity are concerned, the only political issue is whether or not there should be legal requirements of information service providers.

However privacy/confidentiality is another issue entirely. There are legitimate reasons why encounter-derived information should be passed to others. The role of health care institutions is defined not only by their relationship with patients and professionals but

also by the fact that they are corporate entities with their own informatic needs. The former mandates concerns and imposes responsibilities for confidentiality, integrity, quality and availability. At the same time, the community and corporate nature of health care institutions obligates them to access and use some information relating to health care encounters in order to allow them to discharge their obligations to third parties (e.g. government) and to function effectively and efficiently as corporate entities. This generates a new domain of concern arising out of the fear that institutions may stray beyond what is strictly necessary, and may fail to keep these data confidential to those who have a legitimate need-to-know.

Privacy may be breached for other reasons. Statute may dictate that some items of information be reported to appropriate authorities (eg notifiable diseases); a court may so order; concern for the safety of the patient, provider or an identified third party may dictate the need for limited disclosure; and the prevention and detection of serious crime (eg terrorism, drug trafficking) is widely viewed as a reason for selective disclosure. But these are just the tips of various icebergs – where do we draw the line?

The lack of an institutional policy on security matters should give cause for concern.

Back to Top

4.2 Formulating institutional policy, and managing the risks

Institutional policy must be guided by ethical best practice: various recommendations and guidelines on privacy and security exist (eg formulated by OECD) as well as model policies (eg Australian Standard AS….). Policies must take account of legislation (eg relating to Freedom of Information, Privacy, Data Protection), as well as operational realities of the organisation. Security is too important an issue to be left to chance, or to junior staff or even to information services departments: it is a clear obligation of top management and as such they must take an active role in, and be accountable for institutional security policy.

Sections of the policy will lay down, in a form that can be incorporated into contractual agreements:

- Expectations of the institution in terms of its handling of information as a guide to patients and professionals
- Guidelines for clinical and administrative staff, including rules and regulations for the use of the computing systems
- Guidelines for information services staff
- Requirements of external contractors
- Procedures and Penalties in case of suspected breaches of security policy

These policies must be communicated effectively to the various parties, and it is the reponsibility of the institution to ensure that the guidelines are complied with.

Back to Top

4.3 Preventive versus detective security

Conceptually there are two quite different approaches to the management of security issues: prevention and detection. The former is based on the desire to prevent breaches occurring, and involves taking proactive steps to minimise the risks from physical damage and from hostile attack, as well as to limit user privileges to the minimum consistent with the performance of their duties. The latter is based on a *laissez-faire* approach, concerned more with detecting breaches when they have arisen than with preventing them arising in the first place. Most systems have a mix of the two.

However an important perspective is that of the patient: when security has failed, in whatever way and for whatever reason, it is most often the patient who is exposed to risk and who may suffer. Some of the consequences of security breach may be permanent or even fatal: once the breach has happened the damage is done and cannot be undone. A premium must be placed on successful prevention – even so abuses will happen in ways that could not be foreseen or prevented, and it is here that assured detection of abusers is vital.

Approaches to security can be divided into technical and non-technical

Back to Top

---

5. Technical solutions

Technology can address many of the security risks. For example equipment can be sited in secure locations, away from hazard risks such as water, fire, chemicals etc. Continuity of power can be achieved with an un-interruptible power source. The possibility of disk failure can be countered by redundant storage technology (RAID), and of complete system failure by the provision of a back-up system in another location, with a complete mirror of all data and functionality. All these cost money, and the business case must be based on the value and importance of the data to be protected.

5.1 Access control user identification and authentication

All person-based security depends upon being able to identify uniquely every user, and to extend to them the services to which they are entitled, but to restrict access to all other services. Identification and authentication of users, especially from a remote location, is the key to access control, as well as to audit trailing.

Most systems use a combination of userID and password, both items that the user must remember. Passwords must be changed regularly, and are often subject to restrictions, such as no consecutive numbers, inclusion of at least one non-alpha-numeric character and a minimum number of digits. The complexity of these requirements often leads users to write them down, thereby defeating the object of the exercise. Toolkits exist to break access control systems by trying sequentially all the possible combinations.

The other component of access control security are use of a token, and in situations of extreme risk, use of a biometric identifier, such as fingerprint, iris scan or digitised signature. ***Smart cards*** form an ideal tool for this, being a secure token that cannot be duplication, and which can hold other data such as passwords, encryption keys etc.

Back to Top

5.2 Audit trails

Logging accesses to a system, and linking the user identity with all transactions carried out, is an important method of checking whether abuses of privilege are taking place. Audit trails become vital in reviewing changes that may have been made to data and holding those who have made those changed accountable for their actions.

Back to Top

5.3 Encryption and key management

There are two ways of trying to ensure that data is rendered meaningless except to authorised users. One way is to encrypt it, which involves the use of a key and a mathematical algorithm: the other is to split it and store the pieces separately and in such a way that the parts cannot be associated. A key may be of any length, the longer the harder it is to 'crack'. Currently keys are typically between 32 and 256 bits long to provide a reasonable level of security – once again these are too complex for an individual to remember, again suggesting the use of a smartcard.

Encryption is of two forms –symmetric (simple), or asymmetric (complex). Symmetric encryption involves the use of the same key to encrypt and decrypt: once that key becomes distributed it is only a matter fo time before it falls into the wrong hands. Asymmetric encryption involves encryption with one key and decryption with a complementary key. Each user therefore holds 2 keys: one private and known only to that user, and another public and known to everyone. Messages are sent to a recipient encrypted with their public key – these can be read only by the intended recipient who is the sole owner of the complementary private key required to decrypt the message.

Even so encryption can eventually be broken – the more sophisticate the encryption, the more effort is involved, but toolkits exist to crack encryption. However the cost may make it an unattractive proposition.

Back to Top

5.4 De-contextualisation - separation of content and context

De-contextualisation is a particular exemplar of the data splitting approach to security which HIC has pioneered. The principle is that every 'page' of personal material can be separated into context (who, when, where etc) and content (what). The content alone reveals nothing about the persons or institution, and events of the same type are happening every day to different people in one place or another. Content can be kept in readily accessible stores, such as on a world wide web server. The context alone is personal and private, but often not especially sensitive in the absence of any content. It

is the links between the two that are sensitive.

An approach has been developed whereby context and links/pointers to the content can be held on a personal smartcard, so providing the patient with a complete portable medical record. The content can be kept updated by their physicians (who can add new data such as test results to the web-based content record): the patients hold the index and keys to control access to the records.

Back to Top

---

6. Non-technical solutions

Security is not just an issue for technology. There are a number of well-proven non-technical solutions that are highly effective and must be used in conjunction with technology.

The potential limit of these options is that they need proof of abuse before action can follow. That proof will, of course, come from surveillance of the system, through perusal of logs and review of activities. One aspect of the security policy of any computing service provider must be to put in place systematic measures for detection of abuses, and robust processes and procedures for linking those abuses to a specific person.

6.1 User contracts, rules and regulations

First and foremost is the issue of the arrangements between system and service provider and the user. Rules and regulations must be prepared identifying the privileges and responsibilities of the user, and clearly setting down what they may and may not do. In particular security issues must be explicitly addressed in this document. To give this the force of law, the regulations can be embedded in a contract between user and service provider, in which penalties for breach of contract can be specified.

Where appropriate legislation to prosecute acts of abuse or vandalism in the computing system, contracts can readily fill the gap.

Back to Top

6.2 Peer pressure and control

Almost every health professional belongs to one or more professional 'clubs' – specialist associations, local medical groups etc. Each club lays down rules of ethical conduct. Where members fail to follow these rules, the association can take action: that action may be no more than an overt expression of its members disapproval or expulsion from the club. However in medicine peer disapproval can radically affect business, since much of that business is likely to come from professional referrals. Peer pressure is a powerful weapon in controlling the behaviour of individuals, especially where their relationship and standing with their peers is important.

Back to Top
