The Journal Of The International Federation Of Clinical Chemistry
And Laboratory Medicine
eJIFCC

THE SECURITY OF LABORATORY INFORMATIONAND DATA ON PATIENTS

**by David L. Williams,
Editor-in-Chief eJIFCC,
Department of Clinical Biochemistry,
Royal Berkshire Hospital, Reading RG1 5AN, United Kingdom
d.l.williams@reading.ac.uk**
and
**Jonathan Williams
Senior Consultant, MkII Consultancy;
formerly Global Product Manager,
Baltimore Technologies
jmlw001@hotmail.com**

Introduction

Laboratories deal with data on patients that is very sensitive. Even data on ordinary tests must be kept secure and made known only to the requester of the tests (and possibly nowadays to the patient him/herself) and not to anyone who happens to access the results by chance. But the results of some tests, such as pregnancy tests or HIV status, are particularly sensitive and must not be made available to those who have no right to the information.

Legislative background

The area of data protection and data security is a one which has seen significant work in the last few years in many countries and regions. This climate of increased regulation over how organisations acquire, handle and dispose of data is demonstrated by new laws in many countries enacted over the last 10 years.

In the EU the regulation of how personal information is handled started with work on individual data privacy culminating in EC directive 95/46/EC (1). This is a "framework directive" which was then implemented in the legislation of the (then 15) EU member states. Of the provisions of the directive, the requirements on security accuracy and distribution are immediately relevant to laboratory work.

In the UK, the provisions of this directive were included the Data Protection Act (!998) which built upon and strengthened the previous UK Data Protection Act (1984) by incorporating key principles defining the purposes, uses and handling of data relating to living, identifiable individuals. It has recently been updated in the Human Tissues Bill of December 2003.

Laboratory results and their link to patients comes under the definition of 'health record' defined by Section 68 of the Data Protection Act (1998), and means any record which:

consists of information relating to the physical or mental health or condition of an individual, and

has been made by or on behalf of a health professional in connection with the care of that individual.

In addition, in the UK the Human Rights Act (1998) and the Health and Social Care Act (2001) also change the context in which this data security was held.

The United States was without legislation concerned with privacy and data protection until patients were given some degree of protection under the provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (2) in the section "Standards for Privacy of Individually Identifiable Health Information". This Act, which came into force in 2003, imposes similar restrictions on the use of patient data to those in the EU and is a significant step towards world-wide harmonised privacy rights.

Data privacy and laboratory investigations

Data security and privacy is especially important at a number of key stages in its laboratory use:

- how it is captured;
- how it is stored and accessed;
- how and to whom it is communicated.

Each of these stages has specific issues dealt with in the following sections.

Capturing data

It may seem that the capture of data, filling in the request forms and associated specimen paperwork, is the least important step. However, there is a key, obvious, step which may be overlooked: the purpose for which the data is needed.

In almost all privacy or data protection legislation it is incumbent on the data gatherer to explain why the patient is required to provide information (in this case a specimen from which data will be extracted) and the purposes to which it will be put. In most cases this is neglected because it seems obvious that when a patient has provided a blood sample, the purpose is that of running a battery of diagnostic tests.

It is not clear at this stage, however, whether additional tests may be run dependent on the results of the initial tests? Has the patient consented for this information to be used for anonymised epidemiological or research purposes? By designing the capture forms better to make clear and explain the purposes of the investigations to be performed, the patient is better informed and the laboratory has a clear mandate on how to proceed with additional testing.

An example of where this can go wrong is where tests A and B are performed on a specimen but it is later realised that test C is also required - without a clear mandate, some laboratories believe that they cannot perform the additional test. Since the laboratory is typically unable to communicate with the patient, how can it seek or receive the authorisation to proceed. In this case the patient may have to re-attend for a further sample to be collected.

If some laboratories are unclear whether to perform additional investigations for the benefit of the patient themselves, how much less likely is that that they, or their ethical committees, will allow their results, suitably anonymised, for research purposes to the benefit of society. Dr William Lowrance discusses these seemingly-conflicting goals in "Learning from Experience: Privacy and the Secondary Use of Data in Health Research" (3).

Data access and storage

Once the test or tests have been performed on the patients' samples, the results are typically stored on a database or other electronic system.

Ensuring that patient information is secure is achieved by providing:
access only to authorised persons
regular, secure data backups
security of the data from inadvertent communication
security of the data from unauthorised or inadvertent modification

These provisions are fairly common across all electronic systems holding personal data and this section deals with them in a laboratory context.

User authentication

Key to data security provisions is the requirement that information stored in laboratory systems is not accessible by unauthorised persons. In most current systems this is achieved using both physical security (such as the requirement to be at a terminal within a secure area of the laboratory or hospital) and logical security (such as the use of a simple username and password).

In most cases these provisions are adequate. However, periodic review of these systems is the key. Questions which need to be asked are:

Is the system accessible from an external network?

How often are passwords changed?

Where password are used, are they enforced to be "strong" (4) and how often are the required to be changed?

Do users use a single password for all the systems, secure or insecure to which they authenticate themselves?

The authentication of users is a complicated topic in itself; fundamentally it relies on the combination of one or more techniques that can be grouped in the three basic approaches: something the user knows, something the user has, or something the user is. The first is exemplified by the password or passphrase; examples of the second is the smart card or swipe card but the third is rapidly gaining ground as a method of authentication if not identification, the biometric. It seems only a matter of time before simple and swift biometric security is as natural to us as usernames and, combined with a password mechanism, significantly increases data security.

System access

Another potential way that access to patient data can be gained inappropriately is through insecurity of pathology results on computer systems, in the ward, at the general practitioner's surgery or on the laboratory's computers system.

This may be as simple as lack of security regarding paper-based patient notes - it is important to bear in mind that paper records are also generally covered by Data Protection regulations - or automated patient data systems. Again this comes under the general IT security audit

Data backups

It is a widely accepted concept toIT professionals that data is the most precious asset in information systems and, over the past twenty years, backup has become increasingly important. In the US HIPAA covers data backup under its contingency provisions and in EU data protection legislation there is an obligation to preserve and maintain data accurately for the period authorised.

Information leakage and preservation of data integrity

In addition to the authorised channels covered in the next section, patient's information may be inadvertently communicated by authorised users by unconscious execution of malicious code, mistyping or simple human error. Computer users are increasingly becoming aware of the first case as there are increasing numbers of news items where personal and sensitive data has been retrieved from unsuspecting computer users by specially constructed applications now categorised as viruses, trojans and spyware.

In some cases these malicious tools provide data, such as password information, to access other secure sites from which sensitive information is available. This is a good reason to use a second means of authenticating which cannot simply be copied. The best advice to cope with these is to scan personal computers for not only viruses, but spyware too - for more information visit Spyware-guide.com (http://www.spywareguide.com/) or subscribe to one of the commercial scanning solutions (5, 6).

Viruses, Worms and Trojans

In addition to malicious code designed to siphon data some programs are designed to cause damage, use up resources or provide uncontrolled access to systems. There may be many reasons for creating these vandals. However, the potential impact on laboratory systems is significant.

Computer viruses are typically small programs constructed with the purpose of replicating themselves, similar to biological viruses. Viruses typically rely on human intervention to start the infection process, but there have been viruses that have exploited holes in the security of operating systems to distribute themselves to other computers. Some viruses exist within ordinary office applications and some rely on features of the main operating programmes.

In some cases viruses damage files in the process of infecting them. This is extremely unlikely for database-based systems, but fairly common for the files used in general practitioners' offices. In the case of the Laroux virus, which was first detected in 1996, this modifies the values in a spreadsheet which has obvious implications for users of test data.

There are two key lessons to learn:

do not trust any program or data for which you do not know the exact source

even if it is from a trusted source, check that it does not have a virus embedded.

The first lesson is best practice, but in the event that a colleague succumbs to infection, it is vital that this is not spread. The second lesson is what has become essential for all IT users, home or office alike: scanning for viruses. There are many commercial solutions for virus scanning, but most of these have a background component which checks all files as they are "read" or "written" and a less-frequently used component which can check an entire disk exhaustively in a single session.

Worms are a special case of self-replicating viruses in that they spread themselves across networks, the Internet or, more commonly, via electronic mail. Electronic mail became an important vector for infection in the mid-nineties and virus scanning e-mail became a key part of a policy on "Content Security"1. The first major worm struck in 1999, named "Melissa" and those organisations with security solutions were able to continue operations, unlike those without such security. Since then worm incidents have increased in frequency and severity. In addition to desktop virus scanning, since most viruses arrive by e-mail, laboratories should inspect their own electronic mail policy, especially what content is acceptable. To prevent this kind of attack all organisations should scan their e-mail; there are many commercial solutions available to do this.

Trojans are an old form of attack given new life by the capability to connect computers together cost-effectively at high-speed. In essence they draw upon the Greek "Trojan horse" stratagem of sending a seemingly innocuous party into the enemy camp where it then attacks the enemy from within and opens up access to external parties. Computer trojans work by executing unseen, but sending data back to an external destination and in many cases providing access to remote control, or at least expose the user applications. In the case of sensitive data, they are a significant risk; however, they may also be used to capture passwords which may further compromise other systems or networks. The advice to remove trojans is similar to that for viruses – use a good scanner and don't run anything you don't recognise.

For more information on viruses, see the following references (7,8,9,10,11).

Data Communication

Once data is securely held it must fulfil its original purpose, informing the requester for the purpose of diagnosing and treating the patient. This is the final area where it is important that security is maintained and covers: -

Giving out information by telephone, fax or e-mail

Ensuring that printed result reports are delivered only to the person(s) who are allowed to see them.

Providing information electronically to the general practitioner's surgery

Replying to telephoned requests for results

It is sometimes necessary for the requester to phone the laboratory for results of tests that have been requested. It is up to the laboratory to confirm that the results are being reported to the correct person. This can be done in one of two ways: -

The name of the ward or GP practice is taken and the ward or practice is then telephoned from the laboratory. This at least authenticates the destination, if not the individual.

The general practitioner or hospital doctor is given a codeword or password. When that doctor 'phones for a result, he or she is asked for the password and the results are only given to those who give their correct password.

Replying to requests for results via facsimile

The key behind facsimile requests is that the results go to an authorised user. This is more than just checking the destination fax number, but also the recipient. Many laboratories do not provide information via facsimile for the specific reason that it is unclear from the laboratory's perspective whether a transmitted fax could be seen by unauthorised staff. Before using such a system, laboratories should make sure that this method of delivery is secure.

Replying to e-mailed requests for results

Electronic mail is now as ubiquitous in many countries as the telephone was thirty years ago. People naturally believe that if an e-mail claims to be from an individual, it is definitely from them and, even with the news coverage of e-mail virus threats, it is difficult to shake this trust. However it is simplicity itself to forge the sender's name – commonly called spoofing - so that any responses are sent to a third-party.

There are a number of ways to prevent this and a number of tools to accomplish it:

Ensure that staff only send e-mail to known addresses

Train staff to examine the actual destination address of "John Doe" to ascertain whether the destination is valid i.e. a hospital or general pratitioner's address.

Impose a codeword or password system as discussed above

Ensure that all test results contain a codeword (perhaps in the Title of the e-mail) to ensure that those e-mails can be checked against a list of known good addresses either by the local mail client or, more manageably, at a centralised e-mail content security solution

Dealing with printed reports

Reports may be sent by a number of mechanisms including:-
Internal hospital mail systems
Commercial couriers
Postal service

With all of these it is essential that both the recipient and the destination are clearly labelled and the packaging is at least tamper-evident. It is important that data sent to a general practitioner's location is clearly labelled as sensitive and for the attention of the named recipient only. In some practices it is possible that the information will be processed by clerical staff, however these staff are recruited carefully for their discretion and should not be seen as a weak link.

Dealing with computer-based reporting systems

Even when electronic reporting systems are used to provide results, they may be outside the control or influence of the pathology laboratory. The restrictions concerning provision of access only to eegistered and accepted users, hospital staff and general practitioners suitably authenticated using at least passwords, are at least as important. Where this service is delivered via an intranet or the internet, the method of communications should be at least that commonly accepted for e-commerce, namely SSL or it's replacement TLS (12), and should use encryption to at least RC4 with 128-bit keys.

Conclusion

There are many considerations to be made concerning the security of patient data including legislative, ethical, technolgical and operational factors but in general simple measures can significantly reduce the risks of data compromise. By setting out the basis under which tests are performed both with the requester and, through the requester, the patient, the responsibility and authority becomes much more clearly defined. Implementing IT best practice and taking care when defining, and restricting, operational processes ameliorates almost all the areas for concern.

The duty of care for patient information is equivalent to the care a business takes with its financial data – since scandals such as Enron, regulations such as Sarbanes-Oxley are increasing the obligations on the directors for financial reporting, it can be only a short time before personal data security is regarded as having such a high importance.

References

1. European Union - Data Protection – Legislative documents including EC Directive 95/46/EC

(http://europa.eu.int/comm/internal_market/privacy/index_en.htm)

2. US Government - Office for Civil Rights – HIPAA (http://www.hhs.gov/ocr/hipaa/)

3. Dr William W Lowrance, "Learning from Experience: Privacy and the

Secondary Use of Data in Health Research", Nuffield Trust 2002, ISBN 1-902089-73-1

4. Many resources on strong passwords exist including (http://www.microsoft.com/windows2000/en/professional/help/windows_password_tips.htm)

5. Norton Internet Security (Http://www.symantec.com),

6. McAfee antispyware (www.mcafee.com),

7. http://www.microsoft.com/security/articles/virus101.asp

8. Sophos best practice guidelines http://www.sophos.com/virusinfo/bestpractice/

9. http://www.scmagazine.com/

10. http://www.clearswift.com/

11. http://www.trendmicro.com/

12. IETF RFC 2246 (http://www.ietf.org)

(Footnotes)

[1] Coined by Content Technologies, pioneer in the field of e-mail content control.