University of Glasgow

Authorisation of Confidential Data Use and Storage

Information Security Advisory Group

Version 3.0

November 2010

Introduction

This paper explains why authorisation of confidential data use and storage is required and what is required in relation to setting up a College Authorisation Process. It should be noted that data that it is considered inadvisable to place into the public domain (and thus defined as 'confidential' in this document) may none-the-less be discoverable under Freedom of Information legislation which has very tightly drawn exemptions from disclosure.

Objective

Where confidential data are concerned, there are always going to be risks associated with them getting into the hands of people who should not have access to them. The purpose of having a system of authorisation is to ensure that those proposing to hold or use such data have considered the risks in relation to the circumstances of their particular holding and use and put in place appropriate measures to minimise both the likelihood and impact of the risks. Submitting proposals for authorisation provides oversight of that risk assessment and mitigation by an independent party, which helps to protect the proposer, the proposer's School, College and the University from legal action and negative publicity.

College-Based

The circumstances around the holding of confidential data for administrative purposes may well be similar in all areas of the University, but this is not the case in relation to research. It therefore makes more sense for the authorisation to be handled at a College level than at a University level. For research data, in some Colleges, it might make sense for this to be handled as part of ethics approval by the College Ethics Committee, but the circumstances in the different Colleges will vary and different arrangements will be most suited to their needs.

For some corporate services expectations around the handling of confidential information will be set centrally though accountability for the handling of specific data will be at College level (see Generic Authorisation below).

Specific Authorisation

Staff or student research projects that deal with confidential data need to have specific authorisation through the College or University Services authorisation procedures. This is also true for any administrative activities that involve the collection, storage or manipulation of confidential data, unless they are routine parts of a job and the subject of a generic authorisation as described in the next section.

Gaining authorisation involves three aspects:-

- a clear description of what is being proposed;
- an assessment of what risks are inherent in what is being proposed;
- a clear indication of the specific measures that will be taken to mitigate the risks identified.

Those responsible for the authorisation will need to assess if:-

- the project or activity proposed should be taking place and if it is an appropriate way to go about the task;
- the assessment of the risks is realistic and sufficiently comprehensive;
- the mitigation measures are proportionate and are likely to reduce the risks to an appropriate degree.

In any of these assessments, specialist advice may be sought from for example: local IT support, IT Services, The Data Protection and Freedom of Information Office or other services. The final decision is, however, for the Head of College, Head of University Services or those to whom the responsibility for authorisation within a College or University Services has been delegated.

Generic Authorisation

There are activities which routinely involve the use and storage of confidential data where authorisation may be provided for a class of activity with a set of guidelines, rather than requiring authorisation for each instance of the activity.

Within the administrative activities of the University, there is routine use and storage of confidential data. Much of this activity is focussed on central information systems owned by Human Resources, the Finance Office and the Registry and managed by Management Information Services (MIS). These systems are authorised by the management of University Services and there are clear procedures and guidelines as to how the data may be used and who is authorised to have access to particular parts of them. Extracts of these data may be permitted for use in other systems within Colleges and Schools. Any use of these data which involves putting them on memory sticks, CD-ROMs, laptops or sending them by email should be explicitly authorised.

There are therefore activities where it would be sensible to authorise staff with a particular grade or role, carrying out a particular task using confidential data to operate within a explicitly stated set of guidelines as to how they may use and store those data. It is the job of the University Services Departments and Colleges responsible for bodies of confidential data to define the guidelines under which these procedures are authorised and who may operate them.

Risk Assessment

There are a number of formal Risk Assessment Methodologies in existence, each of which have some merit but most are rather cumbersome and mechanistic to apply and don’t necessarily lead to a thorough understanding of the practicalities. What is important is that an assessment of the following four areas needs to be articulated:

1) What is the Nature of the Data?

Confidentiality arises for a number of perhaps overlapping concerns:-

- data that relate to living individuals or that could lead to the identification of a person referred to (directly or indirectly identifying information such as names, addresses, occupations, photographs);
- data given in confidence or data agreed or reasonably assumed to be kept confidential (secret) between two parties that is not in the public domain, e.g. information on business, income, health, medical details, opinion;
- data subject to factors such as ethical guidelines, legal requirements or research-specific consent agreements;
- data which are concerned with security or with other sensitive aspects of organisational operation.

A clear understanding of what elements of the data are confidential and why that is, is essential to understanding what to do about it. Some types of data are so sensitive that a very high level of protection is required, as the consequences of them getting into the wrong hands are extremely serious, whereas for other types of data a low level of protection will suffice. The quantity of data may also be an important factor.

Both the requirements for protection and precaution in the Data Protection Act 1998 and for openness and transparency in the Freedom of Information Act (Scotland) 2005 need to be borne in mind and guidance and assistance from DP & FOI Office should be sought, particularly where there would appear to be a conflict between the two.

2) Where and How is it to be Stored and Used?

Neither the University nor individual staff or students would wish to be the focus of a news story about confidential data being left on memory sticks in car parks, confidential databases on laptops being stolen from parked cars, confidential paper files being inadvertently revealed to the press, CD-ROMs of confidential details going missing in the post, etc. Clearly information held on memory stick, laptops or CD-ROMs or printed on paper all pose risks in relation to their being outside the University. However, information on computers in university offices is also vulnerable to discovery by being left in unattended or unlocked offices and also via the network to which the computer is generally attached.

3) What are the Consequences of Exposure?

These may range from the possibility of a mild rebuke from a regulatory authority, through bad publicity in the local or nation press, withdrawal of accreditation for one or more University activities, loss of confidence in the University by funders, imposition of fines or enforcement notices by the Information Commissioner’s Office, to long complex and costly litigation as a result of a civil or criminal case being brought against the University or an individual. The likely consequences will be one of the factors determining the amount of effort that needs to be put into managing the risk.

4) What Needs to be Done to Mitigate the Risks?

There are a range of precautions that can be taken and what is required will depend on the answers to the other three questions above, ranging from being careful about locking material away and not leaving offices unattended, through encrypting copies of the data that are held on computer media to storing all the data on secure networked data-servers and never having copies on memory sticks, CD-ROMs, laptops or computers in offices. IT Services provides a range of Best Practice Guidance material on its web site at: **http://www.gla.ac.uk/confidentialdata/**.

Record Keeping

Clearly an important part of the authorisation process put into place within a College is its record-keeping. Again there is no desire to be prescriptive as the record-keeping system that is appropriate in one College may not meet the needs of another.

Records need to be kept of:-

- projects or activities that have been authorised, including:-
  - what data are to be stored and used
  - who is permitted to access the data
  - where the data are to be stored
- An asset register should be maintained of the following entities if they contain personal or confidential data:
  - each shared area on a fileserver;
  - each laptop and the name of the person who has custody of it;
  - each removable storage device and the name of the person who has custody of it.

Help and Advice

For many routine authorisations, little specialist expertise is required, beyond whether what is proposed seemed to be sensible and that those proposing it seem to have understood the risks and are to take appropriate measures to contain them. However in some cases those responsible for authorisation may wish to call upon specialist help. This is available from:-

- The Security Team in IT Services.
- The Records Management Service in the Data Protection and Freedom of Information Office.

Appendix - Examples of Different Authorisation Requirements

These examples illustrate a range of data sources/situations which clearly have different requirements with regard to when and when the data are stored and processed and the bodies that should be responsible for authorisation of the specific activity or project, as a result of the level of sensitivity, classification or source of the data concerned.

Admin. 1 Where the University receives a specific *ad hoc* request for confidential information by an external agency regarding a member of staff or a group of staff. The provision of this confidential data would normally be authorised at College level. Central guidance would be provided by the corporate HR Department and the College would be responsible for ensuring that this is followed.

Research 1 Studies involving questionnaires with or without direct contact with the respondents. Student projects are frequently of this type. Such studies would normally be authorisation by the appropriate College Ethics Committee.

Research 2 Studies involving working directly with people (such as patients) or data derived from other areas of professional practice. Where the subjects are patients, such studies are all reviewed by the NHS Ethics Committees, and similar considerations would apply in relation to other areas of professional practice such as Law, Accountancy, etc.

Research 3 Studies where data is being processed on behalf of external bodies and where the nature and sensitivity or classification of the data require a specific ‘Safe Haven’ for security purposes (the Robertson Centre for example or the ECG Core Lab in GRI which handle data that was sent or collected from outside sources). The authorisation of the facility of the arrangements concerning where the data is to be stored and processed is likely to be required by the external body controlling the data, in addition to College ethics approval.

Research 4 Studies involving data which is simply too highly classified or sensitive to be worked with except in the facilities of the originating organisation (such as a Government Department or Military Establishment). A high level of positive vetting of the personnel involved in the study is likely to be a pre-requisite of such work and a rigorous set of conditions are likely to be imposed on the University by the originating organisation.

Appendix – Issues Specific to Clinical Data

Introduction

'NHSScotland Mobile Data Protection Standard v1.0' (29 September 2008) define the following policy:

> *Except when specifically authorised after a risk assessment of the necessary business case: patient, staff or other corporate records shall not be stored on mobile devices including laptops, USB memory sticks, PDA's, Blackberries or any other mobile device or media such as smart phones, CD or DVD.*

It also indicates that, in some cases, storing patient information on a mobile device may be unavoidable for the completion of work duties and the provision of care, and that such cases shall:

1) *be subject to appropriate risk assessment and approval by the local IT security officer;*
2) *meet the security requirements set out in this document; and*
3) *be approved by a Caldicott Guardian.*

Note: It is acknowledged that in relation to the conduct of clinical trials there is a memorandum of understanding between the University of Glasgow and the Greater Glasgow Health Board , which covers such areas as Data Protection and confidentiality. The University Policy on Confidential Data in the University does not supersede any aspects of that MoU.

'Clinical Data' and 'Clinical Records' in this appendix includes all data related to individuals that originates in the NHS and also similar data collected from individuals as part of medical research in the University.

The Role and Responsibility of College Clinical Data Guardian

The role of the College Clinical Data Guardian(s) is to approve the use of clinical information in the College and oversee all procedures affecting access to person-identifiable clinical data. The Guardian(s) would approve the need for such information to be stored digitally and would need to be confident that the data were to be stored according to the Best Practice Guidelines published by IT Services at:- **http://www.gla.ac.uk/confidentialdata/**. The Guardian(s) needs to be supplied with clear information about the specific use and storage of the clinical data, who controls access to the data and under what conditions, and be satisfied that the risk assessment of the research proposal provides a suitable level of protection for the data. Ultimately, the Dean of the College is responsible for data security but the individual(s) appointed as the College Clinical Data Guardian(s) is responsible to the Dean for ensuring that all of the conditions required for data storage and access have been met.

The Guardian(s) has a responsibility to ensure that appropriate record-keeping is in place, which indicates that a specific project had been authorised and specifies the type of data and the nature of the storage. Timescales over which data can be stored also need to be determined and arrangements made for the removal of information and disposal, if appropriate, at the end of a specific project.

Information that constitutes clinical data, NHS business or NHS records should not be stored, transmitted or processed on any University of Glasgow owned or managed computers, networks, servers, desktops, laptops or removable storage devices, or other machines or devices used by staff unless part of a research project authorised by the College via the Clinical Data Guardian(s).