University of Glasgow
Corporate Information Security Policy and
Policy with Regard to Storage and Management of Clinical Data

May 2009

1. Introduction

This document introduces the University of Glasgow Corporate Information Security policy and the on-going University policy with regard to storage and management of clinical data in particular.

The University of Glasgow Corporate Information Security policy relates to all aspects of information security at the University of Glasgow. More details on these and related corporation policies with respect to University IT regulations; Information Security Management System scope; Connection policy for connecting systems to the campus network; Monitoring policy for network and systems monitoring; Incident Handling policy for handling security incidents and breaches of information security policies; Bastion Host policy for the configuration and management of key servers; Guidelines for System and Network Administrators roles and responsibilities of sys and net administrators; Wireless Local Area Network policy for deployment, administration and support of wireless LANs; Password policy - for creating strong passwords; Universal access policy for the provision of Universal access to information resources; Blocking of Network Access - Guidelines and Procedures; Spam Email policy and procedures; P2P Applications; Data Protection; Copyright and Freedom of Information are available at http://www.gla.ac.uk/services/it/regulationscommitteesandpolicies/securitypolicies/.

2. University of Glasgow General Information Systems Security policy

2.1 Purpose

The University Court has legal and other responsibilities to its staff, students and other stakeholders to ensure the security of information assets that it uses and holds, and to ensure the University is not host to threats to the security of information assets elsewhere. Security of information includes the continued confidentiality, integrity and availability of that information. The purpose of this policy is to define the environment in which information will be protected from threats, whether internal or external, deliberate or accidental. Information exists in many forms, and the policy includes the protection of information stored electronically or on paper or in other forms, and in transit whether across the network or otherwise.

2.2 Environment

The University operates in an environment where openness and sharing are valued for many activities, although security is valued for many others. Support resources are over-stretched, but the University is IT-rich. The University will suffer potentially very significant loss of reputation, financial loss or legal penalty however, if its openness allows its IT resources to be used to mount attempted or successful security attacks on others or on its own resources. The University's approach is that the freedom and openness must be balanced by care and responsibility.

2.3 Objectives

The objective of information security is to ensure business continuity and minimise damage by providing controls to mitigate risks and thereby prevent or reduce the impact of security incidents. We are all familiar with the need for security in many aspects of our life, and we all have information which we need to have protected. At the same time we all want to work in an open, free environment. Trade-offs between these objectives are required. The University is required to meet its legal, contractual and other obligations. Therefore the security policy for the University is firstly, that the security (ie confidentiality, availability and integrity) of confidential or important information must be assured, and secondly that the University will provide as open an academic environment as possible, free of all unnecessary controls, to reduce work barriers for staff and the cost of support. The priorities will always be in the order shown, but the relative importance of the two objectives will vary with the

application domain. Nevertheless, the requirement for the first priority means that the security of the network is paramount.

To achieve this requires acceptance by University management and the whole University, of a documented Information Security Management System (ISMS) based on a documented understanding of the risks involved. The scope of the ISMS is documented in the Information Security Management System Scope.

Compliance with the ISMS will help ensure:

- Protection of confidential information including personal data against unauthorised access.
- Integrity of information.
- Availability of information to authorised users when needed.
- Compliance with regulatory requirements.
- Use of University information assets by and for University identified staff and students.
- Business continuity plans.
- Availability of information security training.
- Monitoring and records of security breaches (actual or suspected).

The approach taken is based on BS 7799-2:2002, but the University will not at this stage attempt to register as compliant with that standard, due to the resources that would be required to do so.

This Information Systems Security Policy, when approved by Court, empowers Information Policy and Strategy Committee (IPSC) to approve detailed standards, policies, procedures and regulations to support this policy.

Staff and students who choose not to comply with University regulations and policies in this area will be subject to the University disciplinary policy.

The Secretary of Court has primary responsibility for this policy, and the Director of Information Services is responsible for providing advice to the Secretary of Court and to University Management, and guidance on and support for policy implementation across the University. All Deans, managers and heads of department are responsible for implementing the detailed policies and procedures in their own business areas. Each staff member and student has the responsibility to adhere to such policies and procedures as apply to them. Breaches of this policy and of information security may result in disciplinary action.

3. University of Glasgow Information Systems Security Policy on Clinical Data Storage and Management

Recent concern about the security of patient records in the NHS has resulted in the production of the 'NHSScotland Mobile Data Protection Standard v1.0' (29 September 2008). This describes the minimum standards for the protection of mobile data in NHS Scotland. The standard is primarily targeted at laptops and USB memory sticks. However, the controls are equally applicable to other mobile data devices such as PDAs, Blackberries and removable media. In the context of the standard the University and its computer, networks and data storage may be considered to be a 'mobile device' in that under some circumstances they may be used to store clinical data.

The document then goes on to 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.*

It is clear that the University has a responsibility to mirror these arrangements not only in relation to mobile devices but wherever and whenever clinical data is stored in the University. The policy that follows is aligned with the NHSScotland document, but is intended to cover this wider scope of locations.

3.1 Definition

Clinical Data' and 'Clinical Records' in this policy 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.

3.2 Principles

1) The Data Protection Act 1998 (and subsequent amendments) applies to any storage or processing of clinical data.
2) No clinical data should be on University machines unless explicit approval for a specific project involving those data has been obtained from the relevant Faculty and, if the records originate in the NHS, by the relevant NHS Board.
3) If approval for clinical data has been obtained, the clinical records stored on University machines must be adequate, relevant and not excessive (in terms of variables and cases) to meet the requirements of the specific project.
4) Appropriate organisational and technical measures must be made for the safe storage and use of the data with particular attention paid to security and for its secure disposal or archiving when the project comes to an end.

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 and this policy does not supersede any aspects of that MoU.*

3.3 Policy

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, unless part of a research project approved as indicated below.

Use of any clinical data as part of a research project should be authorised by an academic member of Faculty senior management (as assigned to this role by the Dean of the Faculty). In this policy this role is referred to as the Faculty Clinical Data Guardian and its primary purpose is to evaluate risk assessments of research proposals in order to determine a suitable level of protection for the clinical data.

Authorisation should only be given after a risk assessment has been carried out which covers:-

- an evaluation of the necessity for each item of data (in terms of variables and cases) in the data set in relation to the defined objectives of the research,
- the degree of sensitivity of the data with respect the extent to which it can be linked with individuals (directly or indirectly), the consequences of loss or unauthorised access and whether or not specific protection (as outlined in this policy and associated guidelines) is required,
- the arrangements required for the secure storage of sensitive data so as to prevent it being
  - accessed by unauthorised personnel,
  - lost accidentally (for example on a laptop or on removable media),
  - stolen from vehicles or insecure premises.

Where research involving the use of clinical data, that can be in any way linked to individuals, is approved, a number of controls will apply (including, but not limited to those below) and the Good Practice Guidelines should be followed.

1) It is recommended that data be held **only** on a managed fileserver. Relevant Faculty and Central IT support will configure a shared secure area for this purpose.

2) The data should not be held on local disk storage (e.g. C: drive) of a desktop machine.

3) The data should not be held on a laptop or removable storage device unless this is unavoidable. Any use of data on a laptop should be authorised by the relevant Faculty Clinical Data Guardian (as described above), after a risk assessment of the conditions under which the laptop is to be managed and used has been carried out.

4) Where use of data on a laptop is involved, it is a requirement that a suitably trained member of IT staff should:
   - build the machine as a Standard Staff Desktop machine (including complete wiping of the disk and fresh installation of the operating system)
   - install and configure University-approved full-disk encryption software to protect the data and software. The passwords used to protect data in this environment should conform to the University Password Policy

   It is also recommended that such laptops are purchased through the University approved suppliers as this significantly reduces the chances that SSD environment and encryption software will not work on the machine, which would make it unsuitable to use with clinical data under this policy.

5) Transmission of the data to other parties must be part of a protocol agreed when the project was authorised (or with subsequent approval by the same route) and a risk assessment carried out. This protocol must require such transmission to be via encrypted communications.

6) An asset register should be maintained by the Faculty for the following entities if they contain clinical data:
   - each shared area on a fileserver,
   - each laptop and the name of the member of staff to whom it has been assigned,
   - each removable storage device and the name of the member of staff to whom it has been assigned..

   The register should include:
   - the (base) location of the entity,
   - who is responsible for the management and safe keeping of the entity
   - the name of the project of which the data are part,
   - who has legitimate access to the entity,
   - date of certified deletion (when no longer required for the project – see point 8 below).

7) **All** users of clinical data must sign document the university confidentiality document to indicate that they understand and accept their responsibilities and obligations in relation to clinical data. All those using clinical data must have received appropriate training in:
   - the obligations and responsibilities placed on both the University and individual staff members under the Data Protection Act
   - the use of the necessary security techniques and software

   When any data user changes role or leaves and thus no longer have legitimate need to access the clinical data associated with a project:
   - the appropriate explicit changes in access to systems must be made to ensure that the former user no longer has access,
   - all devices on the asset register for which they have custody should be transferred to a current project member or cleared of the data as indicated at point 8 below.

8) At the end of projects:

- all data must be securely destroyed from laptops, desktop computers or other devices by Faculty or Central IT Staff to ensure that there are no recoverable traces left (IT Staff assigned responsibility for this should sign an appropriately completed form to indicate this has been done before the date of this action is added to the asset register);
- all access to systems holding the clinical data from the project must be terminated;
- project data that is required beyond the end of a project should be archived according a protocol agreed as part of the original project authorisation or by subsequent authorisation.

To support this process, a Faculty Clinical Data Guardian will approve the use of clinical information in the Faculty and oversee all procedures affecting access to person-identifiable clinical data. The Guardian will approve the need for such information to be stored digitally and will need to be confident that the data was to be stored according to the rules outlined elsewhere in the document. This individual will also need to determine who controls access to the data and under what conditions. Ultimately, it is expected that the Dean of the Faculty will be responsible for data security but the individual appointed as the Faculty Clinical Data Guardian would need to be responsible to the Dean for ensuring that all of the conditions required for data storage and access had been met.

The individual would have to keep records indicating that a specific project had been approved and the type of data and the nature of the storage should also be included. Timescales over which data could be stored also need to be determined and arrangements made about removal of information and disposal if appropriate at the end of a specific project.