

Interim Data Handling Procedures

Restricted Processing of Personal Identifiable Information Re: Students and Research Projects

Background

In order to minimise the risk of a breach of patient confidentiality occurring, NHS Greater Glasgow & Clyde (NHSGGC) encrypted all NHSGGC owned laptops/tablets during 2009.

This exercise highlighted a number of laptops which were not owned by us, having been purchased by students from bursary funding or from external funding. These laptops could potentially hold patient identifiable data as part of research projects undertaken by students.

It is likely that the majority of these laptops will not be encrypted however our licensing agreement does not allow us to encrypt laptops which are not owned by NHSGGC.

We are keen to ensure that the risk of a breach of patient confidentiality occurring in this area is minimised.

Next Steps

The Caldicott Guardian and Information Governance Manager will meet with the IT Leads in Glasgow universities to discuss security issues and agree a joint way forward.

These universities are:

- **Glasgow; Strathclyde, Caledonian and West of Scotland.**

Until a formal agreement has been reached the following interim measures will apply to all employees who are registered concurrently as students with a university.

Interim Measures

For the use of personal identifiable data and clinical data in research projects, the following control measures will be put in place with immediate effect:

Personal Identifiable Data

Wherever possible all data must be anonymised before it leaves the clinical environment. If this is not practical, then the minimum identifiable data necessary should be used.

Sending of Data

There are two approved methods for the transfer of the data from the NHS environment to the university or student's own systems:

- Through the use of approved encrypted flashdrives. NHSGGC currently permit the use of SafeStick by Blockmaster. An encrypted USB Flash Drive can be ordered (if authority has been given by a senior manager) by downloading and completing the appropriate form at:

<http://www.staffnet.ggc.scot.nhs.uk/Info%20Centre/Policies/Documents/09Jul02USBAgreement2.doc>

- Through the use of NHSmail which can be accessed over the web outside the NHS environment. Students can either email data to themselves (NHSmail to NHSmail) or attach it to an email (NHSmail accounts can be activated by going to www.nhs.net and following the instructions), save a draft, and then access the draft email to download the data.

Storage of Data

The data may be stored and processed on:

- A university network area that is restricted to the individual who will work on the data plus staff who have a need to access the data (e.g. staff who have to check the academic results, or who are taking part in the data analysis)
- Laptop or home PC with whole disk encryption and from which the data is deleted on completion of the research project
- It is recommended that the hard disk is encrypted with a security application accredited to FIPS 140-2 standard. This standard meets NHS requirements and is recommended by the Information Commissioner's Office. Where no such software is readily available, an alternative may be used, applying the Advance Encryption Standard (AES) as a minimum. (NB: The freely available TrueCrypt software claims to meet this standard: www.truecrypt.org)

**Restricted Use and Processing Agreement
NHS Greater Glasgow & Clyde Data**

Name	
Designation	
Division/Department	
Base	
Contact Details	

Research Project / Audit Title:

User's Declaration:

I declare that I understand and undertake to abide by the Interim Data Handling Procedures on the restricted use and processing of personal identifiable data and clinical data.

Signature: **Date:**