St George's, University of London
Student Handling NHS Data Policy

Purpose

1. The purpose of this document is to provide a clear statement of St George's, University of London's (SGUL) expectations in relation to how students handle NHS Data during the course of their study.

2. The policy is part of the Information Management Policy and applies to all students, including undergraduate and post-graduate taught courses, and students undertaking research degrees, or contributing to research projects at any point during their training.

Information Governance (IG) for Students

3. All students must complete Information Governance training before they have unsupervised access to patients, patient records or other NHS data. Students will be advised of the need to complete the training, and evidence to their year administrator / placement or project lead that they have done so before commencing the project or placement.

4. For course/year cohorts, training will be administered centrally by course teams.

5. For individual students requiring access for research or service improvement projects, the responsibility for ensuring the student is appropriately trained, and that the project has all the necessary approvals before any data collection commences lies with the supervisor. A suggested text for supervisors to send to a student with respect to training is as follows:

    5.1. "Before you start accessing records for this project, you must undertake Information Governance training. You can do this at the following link. All courses are free:

    http://www.e-lfh.org.uk/programmes/data-security-awareness/

    You should do the Data Security Awareness (NHSD) – Data Security Awareness Level 1"

    Print the certificates (usually as electronic/pdf), keep for your own records and show to your supervisor before you start. "

6. Supervisor instructions, and module handbooks should also include this information. Supervisors have a responsibility for ensuring that a record of the training is held by them so that they, if required, can confirm that the training has been completed before the project starts.

7. All audit/service improvement projects should also be registered with the relevant Trust Audit team. Supervisors are responsible for identifying the relevant local mechanism for registration, and ensuring either they or the student have registered the project. Supervisors also have responsibility for keeping records evidencing that registration has happened.

Student held clerking notes, logbooks and records for their own learning

8. It is recognized that as part of their learning, students on many courses will necessarily make and keep notes about patients they have seen, sometimes including information that is inherently personal and sensitive e.g. detailed histories, examination findings, diagnosis. Students must at all times consider whether a living individual could be identified from the data, or, from the data and other information in their possession/likely to come into the possession of others, taking into account that even anonymisation can, if not considered thoroughly, lead to identification. If the answer is YES to potential identification, students must:

    8.1. Always seek consent from patients before obtaining any personal information[1]. Patients are entitled to object to participation in education and training. In some cases, patients may have a formal proxy e.g. where there is a Lasting Power of Attorney in place or where the patient is a minor and consent is sought from a person with parental responsibility. Otherwise, no one other than the patient can give consent.

    Where the patient lacks capacity, you should only seek to access or share patient information if you cannot learn from a patient with capacity to consent. Non-capacitous patients should be involved in learning only when it is necessary and there is no practicable alternative. This is deemed to be ethically and legally possible where care is on-going and the student is part of a team that is properly supervised by a clinician who takes responsibility for the student's interactions. If that is it is considered necessary for the student to participate, the student should record the team with which they were working and the identity (name and role) of the supervising clinician in his or her notes.

    8.2. Record only information that is essential for their learning or the relevant assessment task

    8.3. Anonymise patient information, noting the significance of inadvertently including identifying information, in student records and case studies as far as it is possible to do so, in line with GMC guidance[2]

[1] Includes talking to patients/taking a history, examining them, accessing their results of clinical records, speaking to other family members about them.
[2] https://www.gmc-uk.org Confidentiality: Disclosing information for education and training purposes, items 14 and 15.

Potential Identifier	Recommendations
Name, Gender	Do not use, nor initials. State gender only
Age	No Date of birth, nor age Use age bands (e.g. 3 months for babies/young children, 2 years older children, 5-10y bands adults)
Patient ethnic category	Only if relevant to the case
NHS or Hospital Number	Do Not Use
Dates	Avoid if possible, record minimum relevant information e.g. day X of admission, or truncate to month and year
Location	Avoid if possible (hospital or ward), do NOT use hospital headed paper
Other unique identifiers	E.g. very rare condition, unusual combination of "obvious features", consider carefully if necessary to store at all
Date of Death	Truncate to month and year

9. Ensure any potentially identifiable notes (handwritten or typed, if there are ANY potentially identifiable components) are stored securely (kept or transported in a lockable/password protected device), and potentially identifiable information is redacted or the entire record destroyed as soon as it is no longer required (shredding, confidential waste disposal)

10. Where a student intends to use personal information for an assessment task, e.g. case analysis project, or other report to be shared outside of the NHS team, and it cannot be adequately anonymised, they should obtain written consent from the patient or their representative e.g. an individual with a legally-valid Lasting Power of Attorney to do so. Any audio or identifiable photographic/video information is by definition personal and sensitive, so should only be recorded with written consent.

Data Storage

11. Any identifiable clinical data should be kept only on NHS secure systems, and not transferred under any circumstances to SGUL systems, personal email accounts, personal devices or shared on social media platforms or discussion groups such as WhatsApp.

12. Processing of clinical data, while it is still identifiable, should also only be undertaken on NHS secure systems. This includes pseudonymized data (e.g. spreadsheets / forms with patient data identified by hospital number even if e.g. initials/date of birth etc have been removed). Students should refer to the NHS Business Service Authority Guidance and seek advice from their supervisor if required https://www.nhsbsa.nhs.uk.

13. Fully anonymised data can be exported/transferred to SGUL systems and personal devices for analysis including by email. (NB students and staff won't have any other way; NHS devices won't allow writing to anything other than NHS encrypted data sticks; SGUL BitLocker devices can be read, but not written too on NHS PCs).