



Daily update
(24 September 2026, 8.45am)

Confidentiality and Patient Clinical Records

The focus of this Core Brief is to remind all staff of the importance and necessity of maintaining confidentiality when accessing, using, recording or sharing patient clinical records. This includes staff from Acute Services, HSCP's and Primary Care Services who have access to clinical records as part of their job role.

Patient information is provided in confidence and must only be used for legitimate NHS purposes. Protecting confidentiality supports safe care, maintains public trust and helps NHSGGC meet legal, professional and contractual duties.

A recent story involving NHS Tayside, covered by BBC News, [Data breach investigation into Minnie Merriman's medical records - BBC News](#) has once again highlighted the risks around inappropriate access to clinical records and why the confidentiality of these records is so important:

- Our patients trust NHSGGC with highly sensitive information about their health, care, family circumstances and personal life
- Inappropriate access, use or disclosure can cause distress, harm, reputational damage and loss of confidence in services
- All staff have a duty of confidence, whether or not they have direct patient contact
- Confidentiality is supported by data protection law, professional standards, employment contracts, NHSGGC policies and the Caldicott Principles
- Access to clinical records is monitored and audited. Staff must be able to justify why they accessed a record.

Only access, use or share patient information when you have a clear, lawful and work-related reason to do so. Curiosity, personal interest, concern for someone you know, or informal requests from colleagues, friends or family are never valid reasons to access a patient's clinical record.

Staff responsibilities

- Access patient records only where it is necessary for your role and the task you are carrying out
- Inform your line manager immediately if you have been approached or pressured to access clinical records
- Use the minimum information needed for the purpose required
- Keep information secure, whether it is held electronically, on paper, in emails, on mobile devices or within Microsoft 365 applications

- Do not discuss identifiable patient information in public areas, corridors, lifts, cafes, public transport or on social media
- Do not share passwords, log-in details or system access with anyone else
- Check recipient details carefully before sending patient information by email or other approved systems
- Report suspected incidents, inappropriate access, misdirected information or loss of records promptly via a Datix report
- Complete required information data protection, cyber security and confidentiality training on LearnPro.

Practical do's and don'ts

Do	Don't
Access records only for direct care or another authorised NHS purpose.	Look up your own record, family members, friends, colleagues, neighbours or high-profile patients unless there is a clear authorised role-based reason.
Share information with appropriate staff when needed for safe care.	Share information informally or with anyone who does not need to know.
Use secure approved systems and follow local procedures.	Use personal email, personal devices or unapproved apps to store or send patient information.
Challenge or seek advice if you are unsure whether access or disclosure is appropriate.	Assume access is acceptable because a system allows you to open a record.

Remember the Caldicott Principles

The Caldicott Principles provide a practical framework for handling patient identifiable information. In everyday terms: justify why information is needed, only use it when necessary, use the minimum information required, restrict access to those who need to know, understand your responsibilities, comply with the law, share information appropriately when it supports patient care, and be open with patients about how their information is used.

Consequences of inappropriate access or disclosure

Accessing or sharing patient information without a legitimate reason may lead to investigation, disciplinary action including dismissal, professional referral, legal consequences and loss of public confidence. Even where no information is further disclosed, unauthorised access to a clinical record may still be a confidentiality breach. The Information Commissioner has acted on numerous occasions against individual staff for inappropriate access to records, a recent example can be found here on the ICO website: [Enforcement Action](#)

If you are unsure

If you are unsure whether you should access, use or share patient information, pause and seek advice from your line manager, or contact the Information Governance Team on gqc.dataprotection.generic@nhs.scot

Remember, for all your latest news stories, visit the Staffnet Hub:

[GGC-Staffnet Hub - Home \(sharepoint.com\)](#)



Fighting Flu. It starts with you!

NHS
Greater Glasgow
and Clyde

The flu vaccine is available to
all frontline health and social
care workers and **all** NHS staff.



Find out more



Staff are reminded to make sure their [personal contact details are up to date on eESS](#).

It is important to share Core Brief with colleagues who do not
have access to a computer.

A full archive of printable PDFs are available on [website](#)