

A Unite member update on accessing health and care records

Tuesday 29 September 2026



An introduction to this update

This update is part of several online sessions that we have provided for Unite representatives and/or Unite members in the health service.

Past sessions have been on:

- Annex 31 of the NHS Terms and Conditions of Service Handbook
- How best to write a job description
- The new NHS (in England) staff standards

You can watch recordings of these previous presentations on the Unite in Health website:

<https://www.unitetheunion.org/what-we-do/unite-in-your-sector/health-sector/unite-reps-update-on-the-nhs-job-evaluation-scheme-afc>. You can also listen to the sessions on our podcast channel. This session will also be posted on this page in the next two weeks.



An introduction to this update

There have been an increasing number of cases reported where people who work in health services have accessed health and care records unlawfully. We wanted to provide this session to remind members of their legal and ethical obligations.

Recent cases have included:

- Eleven members of staff sacked by Nottingham University Hospitals NHS Trust for inappropriately accessing medical records of the Nottingham attacks victims [1]
- Nearly 50 staff at Liverpool trust were disciplined for accessing care records of the victims of the 2024 mass stabbing at a dance class in Southport [2]
- NHS staff under investigation after teen's medical records accessed years after death [3]
- HSJ and Sky News recently did a freedom of information request that uncovered a wide scale problem highlighting 200 staff sacked and 2,000 sanctioned [4].
- Unauthorised access to patient records on Encompass investigated across NI trusts [5].

[1] <https://www.bbc.co.uk/news/articles/cgrpdkevvnko>

[2] <https://www.bbc.co.uk/news/articles/cgmpz1mxzd9o>

[3] <https://www.independent.co.uk/news/uk/home-news/nhs-staff-medical-records-oliver-mcgowan-b3055185.html>

[4] <https://www.hsj.co.uk/workforce/exclusive-hundreds-sacked-for-snooping-on-patient-records/8124194.article>

[5] <https://www.belfastlive.co.uk/news/northern-ireland/unauthorised-access-patient-records-encompass-34402776>



An introduction to this update

BBC NEWS

NHS trust sacks staff over attacks victims' records

HSJ

WORKFORCE

Exclusive: Hundreds sacked for snooping on patient records

By Zoe Tidman | 7 September 2026

- Joint investigation by *HSJ* and *Sky News* finds dozens of trusts have no recent or proactive checks for inappropriate record access
- Cases uncovered involve potential domestic violence and a staff member looking at 179 records without legitimate reasons
- Health and social care committee chair says figures paint "stark picture" of issue involving "sacred" data

More than 200 NHS staff have been sacked and around 2,000 others sanctioned for inappropriately viewing patient records over the past five years, *HSJ* can reveal.

BelfastLive

Unauthorised access to patient records on Encompass investigated across NI trusts

"Patients must be able to trust that their most personal information is accessed only when there is a legitimate clinical reason."



INDEPENDENT

NHS staff under investigation after teen's medical records accessed years after death

Oliver McGowan, 18, who had autism and epilepsy, died in 2016 after an antipsychotic medicine triggered a rare reaction and caused his brain to swell



An introduction to this update

Further stories were reported in the weekend before this session which has triggered the issuing of a further letter from Sir Jim Mackey, Chief Executive Officer at NHS England [6].

Dear colleague

You will share my disappointment and anger at the numerous and widespread reports that NHS staff members have accessed confidential patient information without any legitimate reason to do so, [particularly given the new guidance and communications toolkit we launched in July](#).

Unauthorised, inappropriate and unjustifiable access to confidential patient information by NHS employees is unlawful, massively damages patient and public confidence in the NHS and represents a serious failure of our duty to protect the privacy of patients. We all know this is unacceptable and we must do all we can to prevent these incidents.

Patients must be able to trust that their personal information is kept confidential by the NHS and the outrage reflected by the public on this issue is entirely understandable. It is particularly galling that the actions of a minority of staff are tarnishing the reputation of the majority of our colleagues who take pride in delivering the best care for patients.

I have reassured the Secretary of State for Health and Social Care that we intend to take a zero tolerance approach to tackling this problem, driven by a shared understanding across the NHS that, in almost all cases, such unauthorised access to patient records constitutes gross misconduct, and that our actions as employers must now reflect the severity of wrongdoing when patient confidentiality is breached.

Danny Mortimer, Director General for People, has set out updated advice to reflect this new approach in the annex to this letter. Please ensure you implement this approach with immediate effect.

Public confidence in the NHS has improved over the last year in line with the very real improvements we've seen in patient care: this behaviour sets us back and cannot be tolerated. As a leadership community we must now move as one to eradicate it.

Yours sincerely



Sir Jim Mackey
Chief Executive Officer, NHS England

[6] <https://www.england.nhs.uk/long-read/unauthorised-inappropriate-and-unjustifiable-access-to-confidential-patient-information/>



An introduction to this update



Stopping unlawful access to records guidance for health and care professionals

This guidance explains what unlawful access to records is and what organisations can do to keep information safe and check who is accessing health and care records.



[7] <https://digital.nhs.uk/data-and-information/information-governance/guidance/stopping-unlawful-access-to-records/guidance-for-health-and-care-professionals>



What is unlawful access to patient and service user records?

Accessing health and care records out of personal curiosity or for personal reasons is illegal. It causes real harm to patients and service users and could end your career. Everyone working in health and care has a professional and legal responsibility to protect people's confidential information. This includes accessing health and care records only where there is a clear and legitimate reason and doing so in a way that respects individuals' dignity and trust.

Accessing records for any reason other than work purposes is both unethical and illegal. If you are found to have intentionally accessed people's health and care records without an appropriate and approved work reason, you may be committing a criminal offence under the Data Protection Act 2018 and Computer Misuse Act 1990. You may be reported by your employer to the Information Commissioner's Office (ICO) and Police, both of whom have the power to pursue a criminal prosecution.

It is also a serious breach of your employment contract and could result in disciplinary action, including dismissal. It may also result in a referral to your professional regulator and could end your career.



Types of unlawful access

- Access based only on curiosity or personal interest
- Unlawful access for personal use
- Unlawful access with malicious intent
- Unlawful access for incompatible purposes
- Intent to unlawfully access



Types of unlawful access – Access based only on curiosity or personal interest

This is when someone views a record out of curiosity and not because they need to for their job. This may involve accessing the records of:

- friends, family or colleagues
- individuals of local or national media interest
- patients or service users you have seen in the past, when you do not have a current authorised and lawful reason to do so (see the section on Lawful access to patient and service user records)

Personal curiosity is never a legitimate excuse for accessing an individual's health and care record. Whilst you may not have a malicious intent, such actions are a severe breach of confidentiality, privacy and trust and will often cause significant distress for the impacted patient or service user.

Example - A nurse accessed records of people they knew. This included a friend's record to check blood test results because they were curious. The nurse stated they were worried about their friend's health and wanted to check which tests were being done. This is not a valid work reason, it was unacceptable and unlawful.



Types of unlawful access – Unlawful access for personal use

This occurs when someone uses their access to health and care records for a personal reason which is not part of their job.

A common example is when staff members access their own records to check their notes or test results. This can also include accessing the records of friends or family, with their permission, because they want your opinion on their care.

Even if the record is your own, or a friend or family member has asked you to look at their record, you must not use your staff access to view it, unless this is part of an authorised work role and local process. You may see information that would not otherwise be disclosed to you or the person whose record it is, including information that may cause you harm, or which is about another person, and which is confidential. This is considered a breach of confidence, trust and abuse of access.

You can access your own records legitimately through patient facing services, for example, through online patient access services and the NHS App. When you view your information through these services, this access has been approved by a health or care professional who is responsible for treating you and has decided that this information is appropriate to disclose. This protects you and the privacy of other people.



Types of unlawful access – Unlawful access with malicious intent

In some cases, unlawful access can involve malicious intent, such as intent to cause harm. This could include stalking, harassment or causing distress to individuals.

Example - A health worker accessed the records of their ex-partner's family. They used updated contact details to make nuisance phone calls to their ex-partner's family.

Example - Liverpool hospital health worker read in-laws' files

“A former healthcare assistant from Merseyside has admitted illegally accessing medical records of her ex-husband's family so she could make nuisance phone calls...she was convicted under section 55 of the Data Protection Act. She was fined £500 with £1,000 costs. She was also ordered to pay a £15 victim surcharge.



Types of unlawful access – Unlawful access for incompatible purposes

Unlawful access may also occur when someone is allowed to access an individual's record for a legitimate reason (for example, to provide care) but then uses it for a purpose that they are not allowed to use it for.

Example - A clinician accessed a patient's record during treatment and subsequently amended or removed information from the record in order to avoid scrutiny of a clinical decision. Access to the record was authorised; altering the record, for a purpose inconsistent with professional and organisational requirements, was not.

Types of unlawful access – Intent to unlawfully access

This is when a person purposely tries to look at a record they are not allowed to see but the system stops them, for example by blocking their access. These might be identified through routine audit checks or using systems that trigger alerts.



Types of unlawful access – Accessing records following coercion (or similar)

This is not included in the current guidance, but we felt it important to raise as we have come across this issue with members.

Example - A senior clinician insists that you should access a record that you have no reason to access as they want some of the information contained within the record. This could be that they wish to unlawfully access the record for any of the reasons already covered.



Lawful access to patient and service user records

You can access your organisation's health and care records where you have a clear, necessary and authorised work purpose. This includes access for the purposes of:

- direct care (including multi-disciplinary team meetings and necessary clinical follow up after the direct episode of care)
- reflective practice
- resolving complaints, safety investigations and legal action
- morbidity and mortality reviews
- clinical audit and quality improvement
- education, training and teaching
- operational support for care



Types of lawful access

Access to health and care records for legitimate and appropriate work purposes is not unlawful. Health and care professionals, and the teams supporting them, may need to access patient and service user records for a number of legitimate and authorised purposes in addition to delivering care directly to an individual.

Access should:

- have a clear work-related purpose
- be necessary for that purpose
- use no more information than is reasonably required
- be in line with the expectations of the patient or service user
- follow the organisation's relevant policies and approved processes

Where these conditions are met, staff should feel confident in accessing the information they need in order to provide, improve or assure safe and high-quality care. Examples of lawful and permitted access include access for the following purposes...



Types of lawful access - Reflective practice

If you are a regulated health or care professional, you are required to engage in reflective practice as part of your professional regulation. This is considered necessary for the provision of safe and high-quality care and would not constitute unlawful access. This may include reviewing the subsequent outcome of an episode of care in which you or your team were involved, where this is necessary for the provision of safe and high-quality care and is undertaken in accordance with relevant organisational arrangements.

You can read more about using information for this purpose in NHS England's reflective practice guidance [7], reflective practice guidance from professional regulators [8] and the National Data Guardian [9].

[7] <https://digital.nhs.uk/data-and-information/information-governance/guidance/using-information-for-reflective-practice/guidance-for-health-and-care-professionals>

[8] <https://digital.nhs.uk/data-and-information/information-governance/guidance/using-information-for-reflective-practice/guidance-for-ig-professionals#further-information>

[9] <https://www.gov.uk/government/publications/using-data-in-reflective-practice-to-support-safe-care>



Types of lawful access - Resolving complaints, safety investigations and legal action

Where a patient or service user raises a concern or makes a complaint, access to a record may be required in order to:

- support a complaint response
- decide if investigation is necessary
- investigate a patient or service user safety issue
- support an organisational response to legal action, even if you were not directly involved in care

You should follow your organisation's policies and procedures when accessing records for these purposes, including where access to shared or other organisations' records are required. This would not constitute unlawful access.

Types of lawful access – Morbidity and mortality reviews

Individuals and departments may be required to review outcomes for patients or service users in their care as part of morbidity and mortality reviews. This is considered necessary, as part of a learning culture, for the provision of safe and high-quality care. You may also need to access, or support access for medical examiners' or coroners' investigations. You should follow your organisation's policies and procedures when accessing records for these purposes. This would not constitute unlawful access.



Types of lawful access – Clinical audit and quality improvement

If you are a health or care professional, or part of a team supporting them, you may need to take part in a local clinical audit to review care your organisation has provided and check that it was safe and effective. You may need to access records and to follow up with people and offer support or treatment if issues are found. You should follow your organisation's policies and procedures when accessing records for these purposes. Local clinical audit is recognised as part of direct care. Accessing records for these purposes will not constitute unlawful access.

You may also be asked to access records to support national clinical audits and registries or quality improvement initiatives. In most cases access to records for these purposes without a patient or service user's consent needs your organisation to obtain specific legal approval. For example, for national clinical audit, this may need approval from the Secretary of State following an application to the Confidentiality Advisory Group. If you are unsure if legal approval is in place or needed, you should seek advice from your information governance (IG) team. You should also follow your organisation's policies and procedures when accessing records for these purposes. This will also not constitute unlawful access.



Types of lawful access – Education, training and teaching

Learners and educators from any health or care profession may access the records they need where they are providing or supporting care as part of an authorised placement, training role or supervised learning activity. This includes access needed to document the care they have provided and to learn, or in the case of educators, to support learners to learn from that care. It also includes anonymising information so that it can be used as part of training, for example, Radiology Events and Learning Meetings, where cases are discussed to consider radiological discrepancies. Access should be appropriate to the learner's or educator's role, subject to relevant supervision, local role-based access arrangements, and limited to the information needed. This would not constitute unlawful access.

Types of lawful access – Operation support for care

Staff may access the information necessary to coordinate care, manage referrals, identify the right bed or service, manage waiting lists, plan patient or service user flow, arrange appointments, support discharge, or undertake other operational activities that directly support individual care of current patients or service users. Access should be role-based, limited to the information needed for the task, and should not include browsing unrelated clinical detail. This would not constitute unlawful access.



Types of lawful access – Mistakes

If, when performing your role, you access a record by mistake, that will not be unlawful access. For example, you might open the record of a person with the same name as the person you are treating, mistype an identifier, or a clinical system may automatically open a record you did not intend to view. Stop reviewing the record as soon as you recognise the error. If there is a recurring system behaviour or workflow design issue causing this, you should report it to your IT team and your Data Protection Officer (DPO), so your organisation can assess the issue.

Types of lawful access – Other legitimate access

There are several other legitimate reasons to access a record not listed above, for example:

- responding to requests for information from the Police, insurers or other bodies
- the provision of sick notes or equivalent
- undertaking research studies

You should feel confident in accessing a record if you have:

- a clear, justifiable work reason for accessing a record
- your organisation has an appropriate legal basis under data protection laws to process personal data for these reasons, and
- access is necessary and in compliance with your organisation's policies and procedures

If you are unsure, you should speak to your IG team, DPO or Caldicott Guardian.



Consequences of unlawfully accessing records

Unlawful access to records can have a significant impact on individuals and cause harm. People trust health and care providers to keep their information safe. If trust is broken, people might hold back important information. These breaches can affect people's health, personal life and work.

Breaches of confidentiality can leave people feeling deeply distressed, reluctant to use health and care services and prevent them from disclosing information that may help them receive better care.

Accessing records unlawfully could lead to dismissal from your employment for gross misconduct and you being reported to professional regulators, the ICO and the Police. It could end your career.

Accessing health and care records simply out of curiosity or for other personal reasons is illegal and a criminal offence. People who do this have been prosecuted by the Police and the ICO under the Data Protection Act 2018 and the Computer Misuse Act 1990. Committing such offences can result in fines and prison sentences. You will also have a criminal record.



Monitoring access to records

Electronic health and care record systems keep a log of who has searched and accessed which record. Audits of access are routinely carried out. Access that seems unusual or has no clear reason will be investigated and dealt with in line with your organisation's procedures.

Individuals can request information about who has accessed and contributed to their health and care record by making a subject access request (SAR). This means they can review when their record has been accessed and report anything that looks suspicious to the organisation for investigation.

Reporting unlawful access

If you think someone has looked at a record when they shouldn't have, you must report this straight away in line with your organisation's data breach reporting procedures. Unlawful access can in some cases be part of wider criminal behaviour. It also damages trust in health and care services and in some cases, can cause harm to the patient or service user.

If you have concerns about someone unlawfully accessing records or are not sure how to report this, you can speak to your line manager, DPO, IG lead, Caldicott Guardian, safeguarding lead or a Freedom to Speak Up (FTSU) guardian.





The Code

Professional standards of practice and behaviour for nurses, midwives and nursing associates

5 Respect people's right to privacy and confidentiality

As a nurse, midwife or nursing associate, you owe a duty of confidentiality to all those who are receiving care. This includes making sure that they are informed about their care and that information about them is shared appropriately.

10.5 take all steps to make sure that records are kept securely



Your duties as a registrant

Standards of conduct, performance and ethics

5. Respect confidentiality

Using information

5.1 You must treat information about service users as confidential.

Disclosing information

5.2 You must only disclose confidential information if:

- you have permission;
- the law allows this;
- it is in the service user's best interests; or
- it is in the public interest, such as if it is necessary to protect public safety or prevent harm to other people.

10. Keep records of your work

Keep accurate records

10.1 You must keep full, clear and accurate records for everyone you care for, treat or provide other services to.

10.2 You must complete all records promptly and as soon as possible after providing care, treatment or other services.

10.3 You must keep records secure by protecting them from loss, damage or inappropriate access.

