

To: • NHS trust and ICB:

- chief executives
- chief operating officers
- data protection officers

- GP practices
- primary care networks

NHS England
Wellington House
133-155 Waterloo Road
London
SE1 8UG

25 September 2026

cc. • NHS trust and ICB:

- chief people officers
- chief digital information officers
- chief medical officers
- chief nursing officers
- chief clinical information officers
- Caldicott guardians
- senior information risk owners
- communication directors
- chairs

• NHS England regional:

- directors
- chief operating officers
- chairs

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.

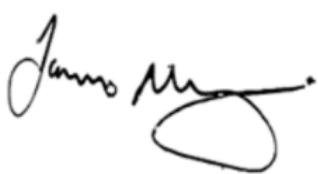
Patients must be able to trust that their personal information is kept confidential by the NHS and the outrage reflected by the public on this issue is entirely understandable. It is particularly galling that the actions of a minority of staff are tarnishing the reputation of the majority of our colleagues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

A handwritten signature in black ink, appearing to read 'Jim Mackey', with a large, stylized loop at the end.

Sir Jim Mackey

Chief Executive Officer, NHS England

Annex A: guidance for trust leaders

According to the [Acas Code of Practice on Disciplinary and Grievance Procedures](#), gross misconduct is an act that is so serious in itself, or has such serious consequences, that it may justify dismissal without notice (summary dismissal) for a first offence. In almost all cases, unauthorised, inappropriate and unjustifiable access to patient records will be unlawful, constitute gross misconduct, and summary dismissal will usually be justified in such cases.

This note provides advice to trust leaders about the best practice approaches to such allegations of gross misconduct. While you must follow your local policies and procedures, you should also review them in light of the advice set out below.

An initial fact-finding element is an essential first step in establishing why colleagues have accessed a particular patient record, whether they were authorised to do so, or whether their act of doing so was inappropriate and unjustifiable. This should be undertaken rapidly.

Where there appears to be a case to answer, you should ensure this is immediately reported to your data protection officer, as it may be a data breach. They may need to report it to the Information Commissioner's Office (ICO) within 72 hours of discovery to meet legal requirements. This should be done through the Data Security and Protection Toolkit reporting tool. Please ensure that your regional director is also promptly alerted to any instances where such breaches in patient confidentiality have occurred.

If there is a misconduct case to answer for any employee, you will need to commence a disciplinary investigation, as per your policy. Unless exceptional circumstances apply, you should strongly consider suspending the employee who is the subject of the allegation for the duration of the process as a neutral act, in order to maintain the integrity of the investigation and minimise the risk of any further breaches. You must follow the specific procedures for the exclusion of medical staff, where relevant.

The act of suspending (or excluding) any employee, while a neutral act, is nonetheless a significant step and the speed, oversight and quality of the investigation should be prioritised by the organisation. Employees' access to relevant patient record systems should also be removed while they are suspended from work.

Where an investigation establishes that there is a case to answer, then a hearing must properly consider all relevant information. Each case will, of course, involve its own aggravating and mitigating factors, which will need to be properly considered.

Rights of appeal will apply as per your policies.

Where it is found that a registered healthcare professional has accessed medical records unlawfully then a referral to the relevant professional regulator will likely be needed and should be actively considered.

You should keep your data protection officer informed throughout the process and of your outcome. They may need to provide information about your response to the ICO. In some cases a report may also need to be made to the police.

There is generally a legal requirement to notify the patient in data breaches of this type under data protection law and as part of duty of candour. The patient should be informed promptly about the breach and what you are doing in response to it. Delays in telling patients and their families when these incidents have occurred can add to their distress.

Where allegations are made against contractors or employees of other organisations with access to your systems, you must notify their employer immediately; you should consider suspending their service and withdrawing their access to your systems and facilities. You should liaise with their employer and provide them with evidence and information about your investigation and support them to take similar action. Where an investigation concludes that the individual accessed a record without authority, you should consider bringing honorary contracts or other arrangements to an end.

Other actions

You should also take appropriate action when high profile incidents occur locally to ensure that the data and access to the relevant records are restricted only to those who need to see them. Please consider what steps you can take to lock down records or flag them to be monitored where there is a high profile incident or patient(s) in your care. If that is not technically possible, then you should ensure you instigate an audit of record access swiftly to identify any unauthorised access and be clear to staff in advance that you will do that.