

- To:
- NHS trust:
    - chief executives
    - chief operating officers
    - data protection officers

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

- cc.
- NHS trust:
    - people officers
    - chief digital information officers
    - chief medical officers
    - chief nursing officers
    - chief clinical information officers
    - Caldicott guardians
    - senior information risk owners
    - chairs
  - NHS England region:
    - regional directors
    - chief operating officers
    - chairs

7 July 2026

Dear colleagues

Patients using NHS services rightly expect their information to be kept secure by the people who treat them. This is why recent reports in the media of staff accessing patient information in unauthorised circumstances are particularly worrying for us all.

These instances may seem like benign curiosity to some, but that couldn't be further from the truth – they are harmful to patients, damage trust and, ultimately, are illegal.

The majority of NHS staff handle patient information responsibly and professionally every day. However, a small minority of individuals undermine the trust that patients place in them and cause unnecessary distress and harm by accessing records without legitimate reason. Aside from the harm caused, these staff members risk their own careers through disciplinary action, dismissal, referral to their professional regulator, and even criminal prosecution.

Every time a breach occurs there is also inevitable and lasting damage caused to public trust in the NHS overall and, specifically, our ability to safeguard people's data – something which

is critical to the long-term future of the NHS as we design technology like the Single Patient Record.

That is why today I am asking trust boards to put a renewed focus on educating staff whilst also implementing a tough approach in response to those who do breach patient trust in this way. There can be no place in the NHS for those who misuse patient information.

### **What we expect from all staff and trusts**

All NHS staff need to understand that accessing patient information for personal reasons isn't just harmless curiosity.

We are today issuing new guidance for staff about unlawfully accessing patient medical history (see Annex A). This is accompanied by guidance for patients on how their records should be used, how they are protected and what they should do if they think their data has been accessed inappropriately (see Annex B). There is also more detailed guidance for information governance (IG) professionals on how their organisations can prevent and monitor for unlawful access to records and the steps they should take when it is identified (see Annex C).

The guidance for staff makes clear that everyone working in health and care has a professional and legal responsibility to protect people's confidential information and that accessing patient records out of curiosity or for personal reasons is illegal.

For employers, if a patient's record has been accessed without a lawful reason for doing so, they must consider reporting it to the Information Commissioner's Office (ICO) and police, both of whom have the power to pursue a criminal prosecution.

Whilst we are determined to address the small number of cases where unlawful access takes place, we also need to focus on preventing this and the guidance for IG professionals covers how arrangements locally can be strengthened and stress-tested. Addressing unlawful access issues requires input and commitment from all areas of an organisation however, including IT teams, IG teams, HR and clinical leaders.

It is important that the content of this guidance is disseminated to staff and that consideration is given to other actions you may need to take to tackle this problem, including ensuring staff handling patient records are appropriately trained, are aware of their responsibilities and the harm that can be caused through unlawful access.

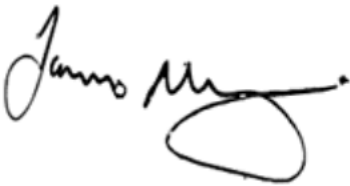
To help educate staff and enforce this messaging, a new campaign with the headline messaging warning: 'Don't let curiosity kill your career' is also being sent to trusts this week (see Annex D). The aim is to remind staff of the law and the potential impact

on patients. Making this messaging as visible as possible through posters and screensavers will support our efforts to ensure patients have the highest levels of confidence in the NHS.

Patient trust in our handling of their most sensitive data cannot be taken for granted and it is therefore critical that we both educate staff and take a hard line when their access to records falls below the standards we expect.

Thank you for joining me in ensuring that these standards are implemented across the country so we can rightly continue to build patient confidence in our use of their data.

Yours sincerely,

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

**Sir Jim Mackey**

Chief Executive Officer

NHS England

**Annex A** – [all staff guidance](#)

**Annex B** – [patient guidance](#)

**Annex C** – [information governance guidance](#)

**Annex D** – campaign brief – document attached