Improving lives

NHS
Sheffield Health Partnership University
NHS Foundation Trust

Board of Directors
Item number: 17
Date: 25 November 2026

Confidential/public paper:	Public
Report Title:	Preventing unlawful access to patient data
Author(s)	Katie Hunter, information governance manager John Wolstenholme, deputy information governance manager and data protection officer
Accountable Director:	Phillip Easthope, executive director of finance digital and performance
Presented by:	Phillip Easthope, executive director of finance digital and performance
Vision and values:	The Trust vision is **to improve the mental, physical and social wellbeing of the people in our communities.** Digital systems allow patient and staff information to be shared and analysed securely to improve clinical decisions, ensuring **(we work together**, **we keep improving)**. Providing equitable access to digital services to all our stakeholders and specific reasonable adjustments when required, ensures **we are inclusive**, and **we provide respectful and kind care**.
Purpose:	To inform the Board of the Trust response to the NHS England (NHSE) chief executive's letters concerning unlawful access to patient data.
Executive summary:	The NHSE chief executive has written to Trusts twice, in July and September 2026, highlighting the need to prevent inappropriate/unlawful access to patient records. This paper presents the current Trust position in this area, informs of ongoing high profile service user access audits and suggests areas for improvement which can be developed in improve our assurance related to unlawful access to records. **Appendices include:** **Appendix 1:** Letter from Sir Jim Mackey July 2026 **Appendix 2:** Letter from Sir Jim Mackey September 2026 **Appendix 3:** Sheffield Health Partnership University (SHPU) EPR legitimate access control summary

Which strategic objective does the item primarily contribute to:					
Effective Use of Resources	*Yes*	✓	*No*		
Deliver Outstanding Care	*Yes*	✓	*No*		
Great Place to Work	*Yes*		*No*	✓	
Reduce inequalities	*Yes*		*No*	✓	

What is the contribution to the delivery of standards, legal obligations and/or wider system and partnership working.

The processes outlined supports compliance with data protection legislation and provides assurance to service-users that their confidentiality is protected by ensuring that their personal information is kept securely and accessed on a need-to-know basis.	
Board assurance framework (BAF) and corporate risk(s):	No specific risks relating to unlawful access are currently recorded on Ulysses, but we have experienced instances of inappropriate access to patient records. Further such incidents are possible, leading to reputational damage to the Trust, loss of service-user confidence in Trust services and the potential for action by the regulator (ICO) or claims for damages from data subjects.
Any background papers/items previously considered:	The paper was presented to executive management team on 1 October 2026.
Recommendation:	Board is asked to: • **Note** the current arrangements for identifying and dealing with inappropriate/unlawful access to service-user records.

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

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

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

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