Inappropriate access to healthcare records

National context and expected practice

NHS England's July 2026 guidance describes access for personal reasons or curiosity as unlawful and harmful, and asks trust boards to renew their focus on staff education and take a tough approach when patient trust is breached. It highlights monitoring and regular audit, role-based controls, limiting access to very sensitive information and multi-factor authentication as relevant safeguards.

The ICO's June 2026 commentary, prompted by high-profile incidents in Nottingham and Southport, states that having the technical ability to view a record is not the same as having a legitimate need. It characterises the issue primarily as a cultural challenge and notes potential consequences including disciplinary action, loss of professional accreditation and prosecution.

DSPT Data Security Standard 4 states that personal confidential data should be accessible only to staff who need it for their current role, that least privilege should apply, and that access should be attributable to individuals. Its guidance also covers assurance, audit scope, logging and monitoring.

Good practice identified

Third-party system access control, linking approval of system access to training, terms and conditions and accountable ownership

Bespoke patient-system training required before access is granted, alongside annual data security training and annual staff Policy attestation

Defining legitimate access through a referral or care relationship, with justification required where no direct relationship exists

Controlled lockdown arrangements and 'break-glass' functionality, supported by Information Governance (IG)/Date Protection Officer (DPO) authorisation and monitoring of emergency access

Logic-based alerts and exception reporting covering clinical systems, to identify inappropriate access patterns, including access to own records, family members, colleagues, high-profile patients, unusual access volumes and access outside normal working patterns

Reviewing patient record access by both individual patient record and staff member, supported by audit trails and contextual information such as working patterns

Monthly review by IG Teams (or equivalent), with findings escalated to line managers and results reported through established governance channels

Recommended actions

Actions
Approve an access monitoring framework Define risk-based monitoring objectives, minimum coverage, frequency, ownership, investigation thresholds and governance reporting. Include EPR, shared care and other systems holding sensitive clinical information.
Introduce proactive and exception-based monitoring Assess current system logging and reporting capability. Prioritise scenarios including access to own records, family or colleagues, high-profile patients, unusual volumes, access outside working patterns and access without an evident care relationship**.**
Establish a high-profile incident protocol Agree how heightened monitoring will be activated, authorised, reviewed and stood down. Use proportionate alerts or lockdown controls while preserving timely access for legitimate care.
Strengthen workforce acknowledgement and communications Require a recorded acknowledgement at induction and system access, supported by periodic reminders and scenario-based communications. Clarify the consequences of curiosity access and routes for reporting concerns.
Standardise investigation, escalation and sanctions Align IG, HR, counter fraud, legal, professional-regulator and police/ICO referral processes. Define decision points, documentation requirements and consistent treatment, while retaining case-specific judgement.

Inappropriate access to healthcare records

Report assurance to the appropriate committee Introduce a periodic dashboard/report covering monitoring coverage, exceptions generated, cases investigated, substantiated breaches, investigation timeliness, outcomes and overdue remedial actions. Avoid reporting identifiable staff or patient details unless necessary.

Develop a capability roadmap Review supplier functionality and options for rules-based analytics before considering AI. Any advanced analytics should have defined purpose, data governance, validation, human oversight and measurable benefits.

Suggested management measures

Monitoring scope	Assurance provided	Suggested reporting metrics
Exception rules operating	Shows detective capability	Active rules and systems covered
Exceptions investigated	Shows operational follow-through	Volume, age and closure rate
Substantiated inappropriate access	Shows realised risk	Trend and category, with safeguards
High-profile events monitored	Shows readiness	Activation and post-event review completed
Access removal timeliness	Shows preventive control	Compliance with locally agreed targets
Training and acknowledgement	Shows workforce coverage	Completion and overdue cohorts

Future benchmarking work

To further support organisations in strengthening controls over inappropriate access to health records, we will be undertaking a benchmarking exercise across our client base to assess the arrangements currently in place, identify emerging themes, and highlight examples of good practice. The findings will be collated and reported in due course.

Further information

Tom Watson
tom.watson8@nhs.net
Alternatively, contact your usual 360 Assurance client manager