INFORMATION GOVERNANCE

Staff Notice

The Information Commissioner has launched an investigation into allegations that hospital staff attempted to view the Princess of Wales's private medical records. This type of incident is not new. Occasionally for personal gain or sometimes just personal curiosity, staff not directly involved, but with system access rights, have been tempted to look at records of famous or newsworthy individuals, and many have been caught doing it.

Do not let curiosity get the better of you!

Data contained within medical records constitutes personal data and accessing such information without valid reason can amount to not only a breach of patient confidentiality, but also a breach of the Data Protection Act (DPA) 2018.

The most common reason that staff break the rules and engage in such behaviour is when they are looking at the medical records for someone they know. Commonly referred to as "snooping," this kind of inappropriate medical records access can lead to actions being taken against staff ranging from internal disciplinary warnings, sanctions from a professional regulatory body, and even criminal prosecution under data protection law.

Electronic records maintain security of data with only staff who have legitimate access being allowed to see them. However, this level is not all that granular, so all the staff on a ward or in a hospital department for example, or at a GP Practice, may have access to a cohort of records but only those who need to use the access are entitled to actually look at a specific patient's record.

In line with data protection and NHS requirements, the Trust must undertake spot checks on who may be accessing sensitive information linked to patients, staff, or their own records. The Information Governance team receive complaints from staff and service users who have concerns that staff may have inappropriately accessed their personal medical records.

We have a process in the Trust to check if staff may be accessing their own medical records and then send out reminders that this should not be happening. Even accessing the record to get your own NHS Number, or checking information is correct, by default will create an audit trail and indicate that you inappropriately accessed information held within the Trust patient record. Please be aware that this is against the **Trust's Confidentiality and Data Protection Policy** because no member of staff is allowed to access their own medical records or medical records of associates (family and friends).

For the attention of:	All staff
Issued by:	Caldicott Guardian and SIRO
In response to:	Local data breaches
Issue date:	April 2024
Review date:	March 2026
Further information contact point:	Trust Data Protection Officer
Alert reference:	IGSN01

Remember, staff accessing medical records must only do so when it is appropriate and required as part of their job and part of what they are working on.

050424MP7519