

Managing inappropriate access to patients' demographic information using IT and local systems and services

This guidance outlines what local health communities should do to prevent, monitor and take action if NHS staff, GPs or GP practice staff use IT systems and services to inappropriately view a patient's demographic information.

Demographic information, including the patient's NHS Number, address and other contact details, is stored on the Personal Demographics Service (PDS). This can be accessed using Choose and Book, the Summary Care Record application, the Electronic Prescription Service and other systems and services that use the PDS to provide patient demographic information. The PDS does not contain clinical information.

Patients' right to confidentiality

It is the duty and commitment of the NHS to keep patients' health information safe, secure and confidential. Patients have a right to privacy and confidentiality and to expect the NHS to keep their confidential information safe and secure, whether that information is in electronic or paper form. Regulatory bodies have also made it clear that they too expect the NHS to put in place the strongest safeguards available.

To maintain privacy and confidentiality, it is a requirement that the new electronic record systems only permit those who have a genuine 'need to know' to access a patient's information, and then only where it is reasonable to believe that the patient concerned would not object, or he/she has been asked for permission.

How do staff access the PDS using IT systems and services?

NHS staff can search for and view a patient's demographic information on the PDS without having an electronic 'legitimate relationship' recorded on the system. A 'legitimate relationship' means the member of staff is working in a team involved in the patient's care. Any member of staff accessing a patient's clinical information must have a legitimate relationship with the patient.

The PDS does not store clinical information; it only stores demographic information. For this reason the PDS does not check for an electronic legitimate relationship when someone tries to access information. This is because people who do not have a legitimate relationship with a patient (ie, are not part of the team providing care for the patient) may still have a justifiable 'business reason' to access the patient's demographic information held on the PDS in order to perform their role.

A justifiable 'business reason' (e.g. as a receptionist in an out of hours setting booking a patient into a local system) is however needed to search for and view patient information on the PDS. This is required to ensure that only those with an appropriate 'business reason' can view a patient's demographic record.

How can local health communities 'see' who has accessed the PDS?

It is possible to see who has accessed a patient's information on the PDS, but not through which programme they accessed it. This is because access to data in the PDS is routinely reported, but how someone accessed it is not.



How can local health communities take steps to prevent inappropriate access of the PDS?

Anyone who has access to search and view the PDS must be approved to do so and must have a business reason for any access.

GPs should exercise due care in their own use of the system and must ensure their staff do not access the PDS inappropriately. The head of the GP practice takes responsibility for this when signing the Information Governance Statement of Compliance (previously known as the Code of Connectivity). In other care settings, the Information Governance Statement of Compliance is usually signed by the trust Chief Executive.

Patients in sensitive or vulnerable positions, for example people who have suffered domestic violence or people in the public eye, may request that their entry on the PDS is flagged as sensitive. This is known as 's-flagging'. When a record is 's-flagged', PDS does not return any of the patient's contact details or other information that could be used to determine their location e.g. address, telephone numbers, GP details.

More information about the PDS and 's-flagging' is available from '[Personal Demographic Service \(PDS\) - A guide for general practice](#)'.

How can local health communities monitor access to the PDS?

Anyone in a local health community can request the following information:

- A report looking at who has accessed a patient's demographic information on the PDS – you can ask for a report to show who has accessed the patient's records
- A report showing which records have been accessed by an individual – all the records that a particular user has accessed

What should local health communities do if they discover someone has inappropriately accessed the PDS?

Inappropriate access can only effectively be policed by the user's organisation. If inappropriate access to any part of a patient's record is discovered, one or more of the following sanctions or actions may be taken against the person who has inappropriately accessed the PDS.

- Criminal action under the Data Protection Act
- Civil action for breach of confidentiality
- Disciplinary action under terms of contract of employment
- Preventing the user from ongoing access to computer systems – this sanction is available to primary care trusts under the terms of GMS/PMS contract with practice
- Action by General Medical Council for breach of patient confidentiality

An investigation into suspected inappropriate access may be initiated by the patient and/or on the recommendation of the employing or supervising organisation's Caldicott Guardian. The particular circumstances of a case will dictate the action taken.

Accessing patient records inappropriately is deemed as personal and, for a clinician, professional misconduct. As soon as inappropriate action is suspected then disciplinary policies and procedures should be used.

