Is an NHS number confidential personal data?

Whilst the NHS Number is not in itself confidential – it is an administrative number assigned by the NHS - for the most part it will be present with other facts about the individual which are confidential and sensitive (e.g. details of diagnosis, social care record and treatment and care plans) and in these contexts, it must be considered both confidential and sensitive. It is also relatively straightforward for many staff to use the NHS Number to identify an individual. Care must be taken to ensure that any processing of the NHS Number which does not meet the requirements of confidentiality law (generally this will be consent) does not reveal anything that is confidential and does not impact adversely on the privacy of individuals.

How can the NHS number be accessed?

It is the intention of the Government for there to be system-wide use of the NHS Number in the context of direct care. The NHS Number is generated and held on the national Personal Demographic Service (PDS) which can be accessed through a range of services. In addition, the NHS number can be made available from local NHS organisations in the context of local partnerships where data protection requirements have been met. In either case, organisations must provide a confidential and secure environment to access these services.

Where the NHS number is made available through a local partnership, there must be an Information Sharing Agreement between the body supplying the NHS Number and the Local Authority or other receiving body, the business purpose must be specific and limited to care, the NHS number is only placed in active records, and the receiving body must be able to demonstrate compliance with confidentiality and security standards through the NHS Information Governance Toolkit.

Systems that provide direct access to the demographic details of registered patients must have a standard of controls including 2-factor authentication, role-based and legitimate relationship models and an audit trail. When systems are to make automated queries of the PDS, a careful set of checks and controls are put into place before the service is enabled.

Communication in the context of direct care will hold confidential information about a client or patient and will include identification of the individual (e.g. name, address) and this set of identifying facts will usually include the NHS number. So the NHS number will be printed on letters, contained within emails and other digital communications (using secure channels - e.g. encrypted email messaging services).

Any organisation or individual receiving any of these communications can only use the NHS number for authorised and lawful purposes. There is however an expectation that the communication or letter is kept securely within the ongoing care record.

---

1 Information Governance Controls for direct PDS access: http://systems.hscic.gov.uk/demographics/pds/ig
Access to PDS: http://systems.hscic.gov.uk/demographics/pds/ig/access
Options for access: http://systems.hscic.gov.uk/nhsnumber/staff/factsheet.pdf
Training in use of the PDS: http://systems.hscic.gov.uk/demographics/pds/training
2 Information Governance Toolkit: https://www.igt.hscic.gov.uk
4 i.e. for direct care and also administration support for care with professional oversight
How should Local Authorities apply the Government Security Classification Scheme (often termed ‘protective marking’) to use of the NHS number?

Local Authorities apply the Government Security Classification Scheme\(^5\) to their information assets. “It applies to all information that is collected, stored, processed, generated or shared to deliver services and conduct business, including information received from or exchanged with external partners”.

The NHS has not adopted the Government Security Classification Scheme, largely because the risk appetite for delivery of NHS services is necessarily different from that of central government but also because all NHS patient data is generally held under strong security measures. Patient data is classed as NHS CONFIDENTIAL by NHS bodies\(^6\). There is a need therefore to map data held by the NHS as NHS CONFIDENTIAL to the Government classification scheme.

There is a subset of the OFFICIAL classification available of OFFICIAL–SENSITIVE for information assets “that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media.”. Such a designation would involve additional procedural and personnel controls to reinforce the principle of “need to know”. When the NHS Number and/or other administrative or demographic details form part of a record or data set that contains confidential and/or sensitive personal data then the classification should be OFFICIAL SENSITIVE.

There is an obligation for all care provider organisations (including private and voluntary sector) to keep patient and client information securely and confidentially. In addition, as stated earlier, there are already stringent controls required for systems which give access to the complete NHS number index.

Can the NHS number be used for “record matching”\(^7\) outside of the controlled NHS computer network (N3 and PSN) such as by private sector care and housing organisations?

Yes, where necessary and only for direct care purposes but the following points should be considered:

- “Record matching” can take the form of looking up a single record as well as comparison of a set of records with those already held on a system. The NHS has a “batch tracing” service available and this may produce better results.
- An individual NHS number can have a status of validated and also verified (Appendix A); these concepts, their significance to safety of care provision, and their local application should be understood before any local matching is initiated.
- The expectation is that all patient and service user identifiers including the NHS number should be appropriately used and be kept secure and confidential; the act of “matching” should not expose the number to loss.
- Information sharing agreements or contracts should ensure that the confidentiality and security standards are clear and complied with.

\(^5\) Government Security Classifications April 2014 - Gov.uk
\(^6\) Guidance for the Classification Marking of NHS Information, Digital Information Policy, Department of Health, January 2009
\(^7\) Record matching is an important process in data integration and data cleaning. It involves identifying cases where multiple database entities correspond to the same real-world entity. In this context the purpose is to populate the records of a database with the NHS number for patients or service users where such usage is appropriate.”