Department of Health

Information governance in relation to local authorities and their new roles in health

Legal basis for use of patient-identifiable data

Any use of personal data, especially if it is sensitive personal data, must be supported by a legal basis for the use of those data.

In practice, the legal basis normally depends on the use of data by a legitimate body for a legitimate purpose, where the purpose requires use of those data in that form.

Examples of a valid legal basis for use of person-identifiable data include:
a. Where explicit consent has been obtained and recorded from the patient or service-user.
b. The processing of confidential information on "communicable disease and other risks to public health" by the Health Protection Agency is supported by Section 3 of The Health Service (Control of Patient Information) Regulations 2002[25].
c. Permission to process confidential patient information has been obtained from the National Information Governance Board under Section 251 of the National Health Service Act 2006[26].
d. The activity may be part of direct patient care and patients would reasonably expect their data to be used for this purpose by this organisation.
e. There is an overriding public interest in the use of such data for this purpose (for example in an emergency) and such use is necessary.

It has been recognised that the current processes for safeguarding personal data are complex and may not always achieve the desired balance between protecting privacy and enabling use for public and individual benefit.

Some significant reforms and reviews are therefore currently in train:
a. The Department of Health has commissioned a review of information governance from the current chair of the National Information Governance Board (NIGB), Dame Fiona Caldicott, to consider the balance between protecting patient information and sharing it to improve patient care. Any changes to the legal framework for information governance in health and care settings will only be considered in light of the Caldicott review, which is due to report later in 2012/13.
b. The NIGB will be abolished from April 2013, when new arrangements will come into place for advising the Secretary of State for Health on applications to access patient identifiable data (commonly

referred to as "Section 251 applications").
c. Under the Health and Social Care Act 2012, the Health and Social Care Information Centre (HSCIC) is required to produce a code of practice covering the collection, analysis, publication and dissemination of confidential information relating to the commissioning and provision of health and social care services in England. The code will build on existing legislation, standards and professional codes of conduct relating to the management, use and disclosure of confidential information, and provide a clear set of guidelines on the sharing, protection and legal disclosure of confidential health information[27]. It will apply both to NHS organisations and local authorities and is expected to be published before the end of 2012.

To enable public health teams based in local authorities to provide population health advice there must be an appropriate information governance architecture in place agreed with local partners. Where required, this architecture will allow public health teams to receive, store and analyse patient identifiable and record-level data.

However, aggregate or anonymised data will be sufficient to meet most public health intelligence requirements, and confidential information should only be accessed in instances where this is absolutely necessary and there is no practical alternative.

The new HSCIC will, in due course, provide access to a wider range of de-identified and linked datasets, which will meet many of the needs of local authorities. In terms of local data, commissioning support units and data management integration centres provide a possible future option for local authorities to obtain record-level data.

If local authority-based public health intelligence teams are going to handle record-level or other patient-identifiable NHS data they will need to demonstrate compliance in with level 2 of the Hosted Secondary Use Team/Project version of the NHS IG toolkit, and the presence of a "safe haven"[28] arrangement.

Local authorities already working with the Social Care Delivery, Local Authority or other versions should contact the IG toolkit helpdesk (0845 3713671); exeter.helpdesk@nhs.net) for advice on how their current assessment may be extended to cover their new public health responsibilities.

Public Health England will work with partners including the HSCIC during 2012/13 to develop a national checklist for information governance arrangements at the local level, which local teams may use to inform local agreements.

IT architecture: the boxes and wires and what goes down them

The most widely used secure network within the health sector is the NHS National Network, known as N3[29], while most primary care trust-based public health staff use its secure email system NHSmail for transfer of sensitive data.

Public health intelligence teams based in local authorities are likely to need to be connected to N3 in order to fulfil their function.

This would only not be required if the authority was very extensively supported by a health intelligence function in another organisation.

Limited access to essential data because of the lack of appropriate IT architecture (N3 connectivity in particular) has been identified as a formal risk by the Public Health England Programme Board.

N3 is intended to provide connectivity to an organisation formally recognised as "delivering health services", and at least 40 local authorities in England have already arranged access to N3 on this basis.

A local authority wanting to connect to N3 has to go through a process known as "Information Governance Statement of Compliance". This is the process by which organisations enter into agreement with NHS Connecting for Health for access to its services, including the NHS National Network (N3).

The terms and conditions of access are set out in the IG Assurance Statement, which is a required element of the IG toolkit[30].

Alternatively, connection between local authorities and the NHS can occur through the Government Connect Secure Extranet, or GCSX. This is a wide area network (WAN), which enables secure interactions between connected local authorities and other Government Secure Intranet (GSi) connected organisations[31].

The Government has also developed a "Public Service Network" (PSN) strategy. PSN is a "secure private internet" for the public sector – it is like the internet but with the security that the government requires[32].

The rationale is that most departments, agencies, local authorities, police authorities etc have their own network. At least 2,000 networks exist, connecting around 5.5 million public sector workers over hundreds of sites.

The aim of PSN is to work with these bodies to rationalise and standardise the networks. Ultimately all public sector networks will be connected, and each government department should already have an established roadmap for implementation. In London 11 boroughs have added the N3 service to their London PSN infrastructure.

IG toolkit completion remains a requirement for whoever wishes to access confidential data.

Finally, an alternative possibility is for individual health workers to request a virtual private network (VPN) token to access N3. A single user VPN enables access to the N3 network via the internet[33].

There are therefore a number of options for gaining access to N3 from a local authority base. None is completely straightforward, and it is imperative that local authorities that have not done so address the issue of access to N3 as soon as possible.

NHSmail

NHSmail is the national email and directory service available to NHS staff in England and Scotland. Accredited to Government – RESTRICTED status, it is the only NHS email service secure enough for the transmission of confidential patient information.

The Department of Health information strategy has stated[34]: "All e-mail communication about our care must be appropriately secure and protected. Work will continue to improve access to and use of NHSmail within the NHS, and social enterprises and other qualified providers of care services, as part of their commissioning contracts with the NHS, will be given access to a limited number of NHSmail accounts. Similar incentives for social care will be made available that make the process and cost of connecting social care providers, local authorities and other care providers via secure electronic communication easier, cheaper and less bureaucratic."

The use of NHSmail relies on a number of features: role-enabled access; appropriate administrative support including funding; the holding of certain software licences; and compliance with information governance requirements:
a. Role-enabled access: NHS staff are enabled to apply for an email account with NHSmail on account of their employee status. Connecting for Health in general agrees to the use of NHSmail by non-NHS organisations provided that the business purpose is health.
b. NHSmail service is provided centrally free-of-charge, although there may be a requirement for local administration as part of ordinary IT management.
c. Specific software licenses are also required to use NHSmail eg Windows Server 2003 and Exchange Server 2007 client access licences purchased under the Microsoft PSA09 agreement[35]. Connecting for Health is enquiring whether existing licences can be transferred to the local authority.
d. Information governance requirements: see above.

A number of public health intelligence teams who have already transferred to local authorities have maintained access to their NHSmail accounts.

[25] www.legislation.gov.uk/uksi/2002/1438/contents/made

[26] www.legislation.gov.uk/ukpga/2006/41/contents

[27] See Department of Health. NHS Information Governance - Guidance on Legal and Professional Obligations, 2007 (www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616)

[28] A "safe haven" in this context is defined as the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. (www.connectingforhealth.nhs.uk/systemsandservices/infogov/igfaqs/safehaven/view)

[29] N3 is the National Network for the NHS. It provides a broadband network, supporting IT infrastructure, networking services and sufficient, secure connectivity and capacity to meet current and future NHS IT needs. With the exception of specific applications information is unencrypted when transmitted within N3. Confidentiality of sensitive information in transit over N3 is not assured, and Department of Health guidelines stipulate that patient-identifiable data must be kept confidential. It is the data owners' responsibility to ensure appropriate controls are in place to secure data in transit. Connection and router are both supplied and managed by the N3 Service Provider (N3SP). www.connectingforhealth.nhs.uk/systemsandservices/n3

[30] www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/non-nhs

[31] www.buyingsolutions.gov.uk/services/Communications/GSi

[32] www.cabinetoffice.gov.uk/resource-library/public-services-network

[33] http://n3.nhs.uk/ProductsandServices/N3Connectivity/ConnectAnywhere%28remote%29.cfm

[34] http//:informationstrategy.dh.gov.uk

[35] www.connectingforhealth.nhs.uk/systemsandservices/nhsmail/using/third

Actions

- Local authorities will wish to understand whether and what need there is for access to confidential data by health intelligence teams for defined purposes.
- The Public Health England Transition Team is working with the Association of Directors of Public Health to develop a list of examples in which directors of public health may need access to confidential data.
- Public Health England will work with partners including the HSCIC during 2012/13 to develop a national checklist for information governance arrangements at the local level, which local teams may use to inform local agreements.
- For confidential data access, local authorities will need to meet the Information Governance Toolkit level 2 in having a safe haven architecture.
- Local authorities will wish to consider how to connect to N3 and to establish NHSmail accounts for all local authority staff engaged in public health commissioning (which may be broadened to social care in time).

DH Department of Health

Produced: September 2012

Gateway reference: 18033

Produced by the Department of Health
www.dh.gov.uk/publications