Information Governance and Caldicott Principles: an overview

Dr Tom Chan

Senior Research Fellow

Section of Clinical Medicine and Ageing

Faculty of Health and Medical Sciences

www.surrey.ac.uk

Privacy

Privacy - a concept going back to the beginning of recorded history – the ability of an individual or group to seclude themselves, or information about themselves, thereby express themselves selectively

The boundaries of what is private differ among cultures and individuals with shared common themes (e.g. the right to be let alone, secrecy, autonomy, self-identity, bodily integrity etc.)

In Western culture, individual privacy - the right not be subjected to unsanctioned invasion of privacy by government, corporation, journalists or individuals is part of privacy laws, including:

- Political privacy – voting systems, secret ballot as a basic right in democracy
- Information privacy – evolving with advances in technologies
- Financial privacy – financial transactions are guarded against fraud and identify theft
- Internet privacy – the ability to reveal or withhold information over the internet
- medical privacy – protect health information, sexual privacy

However, all countries have laws which limit privacy – e.g. taxation, public interests, notifiable diseases & national security

This presentation is principally concerned with medical privacy

Data Protection Act 1998:

An overview

In the UK – privacy is enacted within Data Protection Act 1998, which bring British law in line with EU Data Protection Directives 1995: -

- Defines UK law on the processing of data on identifiable living people
- Governs the protection of personal data in the UK
- The Act applies only to data which is held on computers or in a 'relevant filing system'
- Anonymised or aggregated data is not regulated by the Act (provided anonymisation or aggregation is not reversible)
- Outlines eight principles of good information handling

DPA: Personal information

Personal data means data which relate to a living individual who can be identified –

- (a) from those data (e.g. name, address, telephone number, email address), or
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
- Health records relating to deceased people do not carry a common law duty of confidentiality.
- However, DoH and GMC policies - records relating to decease people should be treated with the same level of confidentiality as those relating to living people

DPA: Sensitive personal information

Sensitive personal data means personal data consisting of information as to –

- the racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of a similar nature
- member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- physical or mental health or condition
- sexual life
- the commission or alleged commission of any offence by data subject, or
- any proceedings for any offence committed or alleged to have been committed by data subject, the disposal of such proceedings or the sentence of any court in such proceedings

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data

Data Protection Act 1998:

The eight principles

There are eight principles of good information handling outlined in the Act :

1. Fairly and lawfully processed
2. Processed for limited purposes - process the data in a way that is compatible with your original purpose(s)
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Handled according to people's data protection rights
7. Keep safe and secure - appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Not transferred to other countries outside EEA without adequate protection

DPA: Data Processing

DPA regulates the “processing” of personal data -

Processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data,
- Retrieval, consultation or use of the information or data,
- Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- Alignment, combination, blocking, erasure or destruction of the information or data.

The DPA definition of processing is very wide, difficult to think of anything an organisation might do with data that will not be ‘processing’

Rights and obligations under the Data Protection Act

There are 3 broad groups of people referred to in the Act: -

- **Data subjects** – individuals about which data is held – i.e. everyone
- **Data users** – person who make use of personal information for a certain purpose
- **Data controllers** –a legal entity (person or organisation) in charge of collection and use of personal data, e.g. your general practitioner
  - **Data controllers** determine the purposes for which and the manner in which any personal data are processed
  - **Data processors** means any person (other than an employee of the data controller) who processes the data on behalf of the data controller, Data controllers remain responsible for ensuring their processing complies with the Act

Data Protection Act 1998:

Conditions relevant to the first principle – Personal data

What is lawful –

The Data Protection Act does not define. However, “lawful” refers to statute and to common law, whether criminal or civil.

Processing may also be unlawful if it results in:

- a breach of a duty of confidence. Such a duty may be stated, or it may be implied (e.g. medical or banking information)
- an infringement of copyright
- a breach of an enforceable contractual agreement
- a breach of industry-specific legislation or regulations
- a breach of the Human Rights Act 1998, among other things, gives individuals the right to respect for private and family life, home and correspondence

Data Protection Act 1998:

Conditions relevant to the first principle – Personal data

Personal data should only be processed fairly and lawfully- in order for data to be classed as 'fairly processed', at least one of these six conditions must be applicable to that data (Schedule 2).

- The data subject has consented* to the processing
- Processing is necessary for the performance of, or commencing, a contract (to which the data subject is a party)
- Processing is required under a legal obligation (data controller is subject)
- Processing is necessary to protect the vital interests of the data subject
- Processing is necessary to carry out any public functions
- Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject)

* Consent - according to EU Directive:

"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

Non communication should not be interpreted as consent.

Data Protection Act 1998:

Conditions relevant to the first principle – Sensitive personal data

- Sensitive personal data should only be processed fairly and lawfully - at least one of the conditions in Schedule 2 is met, and at least one of the conditions in Schedule 3 is also met: -
- The individual has given explicit consent to the processing
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of:
  - the individual or another person *
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

DPA: rights of data subjects

Personal data shall be processed in accordance with the rights of data subjects under the Act (the sixth data protection principle):

- right of access to a copy of the information comprised in their personal data
- right to object to processing that is likely to cause or is causing damage or distress
- right to prevent processing for direct marketing
- right to object to decisions being taken by automated means
- right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- right to claim compensation for damages caused by a breach of the Act

Data Protection Act 1998:

Some exceptions

The Act provides a number of exceptions, including:

- Protection of national security is exempt from all data protection principles
- Prevention or detection of crimes, and assessment or collection of taxes are exempt from the 1st principle
- Domestic purposes – processing by an individual only for the purposes that individual's personal, family or household affairs is exempt from all principles. For example – keeping a database of addresses, dob of family and friends; digital camcorder of family holiday which include people they meet on holiday
- Journalism, literature and art - exempt from most provisions of the DPA, including subject access – but never principle 7 (unlawful obtaining of personal data)
- Publicly available information - where an organisation is obliged by or under an enactment to make information available to the public, personal data that is included in that information is exempted

Information Governance

Health care settings

- Health records are confidential - shared only on a need-to-know basis
- Legal frameworks and national and professional guidance in data security and data sharing are complex in the UK. Relevant legislations include: -
  - Common law
  - Human Rights Act 1998
  - Section 251 of the NHS Act 2006
  - Access to Health Records Act 1990
  - And many more
  - Crime and Disorder Act 1998
  - Freedom of Information Act
  - The Care Act 2014
  - Mental capacity Act
- A number of initiatives to summarise these Legal frameworks & guidance into: -
  - A set of principles – e.g. Caldicott principles
  - A code of practice – e.g. Code of practice on confidential information
  - Auditable standards –e.g. NHS Information Governance toolkit

Caldicott Review:

- Largely due to the development of IT in health services, a review was commissioned in 1997 by the Chief Medical Officer of England to address:-
  - Increasing concern about the ways in which patient data is being used in the NHS
  - Ensure that confidentiality is not undermined
- A committee was established under the chairmanship of Dame Fiona Caldicott
- Caldicott Report in 1997 highlighted 6 principles
- These principles were subsumed in the NHS confidentiality Code of Practice 2003
  (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf)
- In 2012, Dame Caldicott produced a follow up report and added a 7th principle

Caldicott Principles

1. Justify the purpose(s)
   Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian, the Caldicott Guardian.
2. Don't use patient identifiable information unless it is necessary
3. Use the minimum necessary patient-identifiable information
4. Access to patient identifiable information should be on a strict need-to-know basis
5. Everyone with access to patient identifiable information should be aware of their responsibilities
6. Understand and comply with the law
   Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
7. The duty to share information can be as important as the duty to protect patient confidentiality
   Official policies should support them doing so.

NHS Information Governance Toolkit (IGTK)

- Information Governance (IG) ensures necessary safeguards for, and appropriate use of, patient and personal information.
- IGTK - DH Policy delivery vehicle, NHS Digital to develop and maintain
- It draws together the legal, national and professional guidance and presents them in in a single standard
- Organisations that have access to health and social care information must provide assurances that they practice good information governance
- Use IGTK to evidence this - submitted online by 31 March each year.
- Three comment themes: -
  - Management structures and responsibilities (e.g. assigning responsibility for carrying out the IG assessment, providing staff training, etc.)
  - Confidentiality and data protection
  - Information security
- Four attainment levels: 0, 1, 2, and 3 for each criteria (minimum pass at level 2)
- https://www.igt.hscic.gov.uk/requirementsorganisation.aspx?tk=427494475892491&cb=8da925d8-fb2b-4bd1-804e-83ca913cf521&lnv=2&clnav=YES

Information Governance Management	
14-120	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff
14-121	There is an information governance policy that addresses the overall requirements of information governance
14-122	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.
14-123	All staff members are provided with appropriate training on information governance requirements.
Confidentiality and Data Protection Assurance	
14-220	Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected
14-221	There are appropriate confidentiality audit procedures to monitor access to confidential personal information
14-222	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines
14-223	All transfers of personal and sensitive information are conducted in a secure and confidential manner
Information Security Assurance	
14-330	Policy and procedures ensure that mobile computing and teleworking are secure
14-331	There is an information asset register that includes all key information, software, hardware and services
14-332	Unauthorised access to the premises, equipment, records and other assets is prevented
14-333	There are documented incident management and reporting procedures
14-334	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate
14-335	There are adequate safeguards in place to ensure that all patient/client information is collected and used within a secure data processing environment (safe haven) distinct from other areas of organisational activity.

UNIVERSITY OF SURREY

Requirements for Hosted Secondary use team/ project

www.surrey.ac.uk

The National Data Guardian's Review of Data Security, Consent and Opt-Outs

- September 2015: Secretary of State for Health commissioned a review of current approaches to data security across the NHS
- The National Data Guardian (NDG), Dame Caldicot, working with Care Quality Commission (CQC), is asked to conduct the review and to propose
  - a set of data security standards applicable across the NHS *and* social care system and method to assess compliance with CQC
  - new model of consent /opt outs
- The NDG's review report was released in June 2016 - called for local leadership to strengthen the role of Senior Information Risk Owner and Caldicott Guardian
- Three pillars of information security: people, process and technologies
- The recommendations are undergoing a period of consultation

The National Data Guardian's Review of Data Security, Consent and Opt-Outs

- The review endorses there existing right that patients are able to opt out from their confidential information being shared beyond their own care as guarantee by the NHS Constitution.
- The opt-out of course does not apply where there is a mandatory legal requirement or overriding public interest such as notifiable diseases, child or vulnerable adult safety purposes.
- The review is consulting on whether the opt-out choice could be in two parts:
  - Opt-out of their data being used for purposes connected with running of the NHS and social care system
  - Opt-out of their data being used to support research
- A recommendation of the report is that 'opt-outs' should not apply to all data flows to the statutory safe haven of NHS Digital. NHS Digital will link, de-identify or anonymise and share it with those that need to use it – with stronger sanction to protect anonymised data

Some references/resources

- Department of Health: Information Governance Toolkit https://www.igt.hscic.gov.uk/
- Di Iorio CT, Kuziemsky C, Liaw S, Chan T, de Lusignan S, Lo Russo D. The UK National Data Guardian for health and care's review of data security, consent and opt-outs: leadership in balancing public health with rights to privacy? *J Innov Health Inform*. 2016;23(3):620–624.
- Health and Social Care Information Centre, Code of practice on confidential information September 2014 http://systems.digital.nhs.uk/infogov/codes/cop/code.pdf (accessed on 22/08/2016)
- National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs. June 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
- The Caldicott Committee. Report on the Review of Patient-Identifiable Information. Dept of Health; Dec 1997
- https://ico.org.uk/for-organisations/guide-to-data-protection/