Information Governance and Data Security

Version 3.0 2018

Aligned to the UK CSTF

Objectives

The learner will:

- Understand the principles of Information Governance and the importance of data security in health and care
- Understand the different types and values of information
- Understand the principles of data security, including how to ensure the confidentiality, integrity and availability of data
- Understand the principles of data security, including how to ensure the confidentiality, integrity and availability of data
- Be aware of threats to data security and know how to avoid them, including:
    - Social engineering
    - Using social media safely
    - Using email safely
    - Malicious software
    - How to protect information
    - Physical security
- Be able to identify data breaches and incidents and know what to report
- Understand fundamentals of data protection and the General Data Protection Regulations (GDPR)
- Understand the Caldicott Principles and be able to provide a confidential service to patients and service users
- Understand the responsibilities of healthcare organisations under the Freedom of Information Act 2000
- Understand individual responsibilities in responding to a Freedom of Information request

Introduction

Every patient should feel confident that information about their health is securely safeguarded and shared appropriately when that is in their interest. Everyone working in the health and social care system should see information governance as part of their responsibility. The Care Quality Commission states that Patient safety can only be assured when information is accessible, its integrity is protected against loss or damage, and confidentiality is maintained. Data security should be treated very seriously.

Obligations on Individuals Working in the NHS

All staff should meet the standards outlined in this document, as well as their terms of employment (or other engagement agreements). Much of what is required builds on existing best practice. What is needed is to make this explicit and to ensure that everyone strives to meet these standards and improves practice.

Clearly staff are constrained from meeting these standards where appropriate organisational systems and processes are not yet in place. In these circumstances the test must be whether they are working within the spirit of this code of practice and are making every reasonable effort to comply.

The need for change may apply to many existing systems and processes and it is important that staff know who – perhaps the Caldicott Guardian or information governance lead – should be informed of any specific problems or barriers to change that are noted.

Information: To share or not to share? The Information Governance Review March 2013 Department of Health

People using health and social care services are entitled to expect that their personal information will remain confidential. They must feel able to discuss sensitive matters with a doctor, nurse or social worker without fear that the information may be improperly disclosed. These services cannot work effectively without trust and trust depends on confidentiality.

However, people also expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service. So good sharing of information, when sharing is appropriate, is as important as maintaining confidentiality. All organisations providing health or social care services must succeed in both respects if they are not to fail the people that they exist to serve.

The term used to describe how organisations and individuals manage the way information is handled within the health and social care system in England is 'information governance'. In 1997 the Review of the Uses of Patient-Identifiable Information, chaired by Dame Fiona Caldicott, devised six general principles of information governance that could be used by all NHS organisations with access to patient information. The chapter sets out those principles, which have stood the test of time.

It explains why the 1997 review gave priority to discouraging the uploading of personal information on to information technology systems outside clinical control. The issue of whether professionals shared information effectively and safely was not regarded as a problem at the time.

NHS organisations responded by appointing 'Caldicott Guardians' to ensure that information governance was effective. The practice spread to other public bodies, including local authorities and social care services, and the remit of the guardians was extended to provide oversight of information sharing among clinicians.

Over recent years, there has been a growing perception that information governance was being cited as an impediment to sharing information, even when sharing would have been in the patient's best interests. In January 2012 the NHS Future Forum work stream on information identified this as an issue and recommended a review "to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care".

The Government accepted this recommendation and asked Dame Fiona to lead the work, which became known as the Caldicott2 review.

The introduction sets out how the review has been conducted and puts it in the context of the Government's Information Strategy, the Health and Social Care Act 2012, the Open Data White Paper, the review of the NHS Constitution and other relevant initiatives.

The Six Principles

The Caldicott principles refer to a review chaired by Dame Fiona Caldicott in 1997. The Review of the Uses of Patient-Identifiable Information, devised six general principles for information governance that could be used by all organisations with access to patient information:

1. **Justify the purpose(s)** Every 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.

2. **Don't use patient identifiable information unless it is absolutely necessary** Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary patient-identifiable information** Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to patient identifiable information should be on a strict need-to-know basis** Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. **Everyone with access to patient identifiable information should be aware of their responsibilities** Action should be taken to ensure that those handling patient identifiable information — both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law** Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

Protect Patient Information

Patients' health information and their interests must be protected through a number of measures:

- Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality;
- Recording patient information accurately and consistently;
- Keeping patient information private;
- Keeping patient information physically secure;
- Disclosing and using information with appropriate care.

Patients' health information and their interests must be protected through a number of measures:

Recognising that confidentiality is an obligation for all staff, external contractors, and volunteers.
The duty of confidentiality arises out of the common laws of confidentiality, professional obligations, and also staff employment contracts (including those for contractors). Breach of confidence, inappropriate use of health records or abuse of computer systems may lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings. Staff should ensure that they are aware of the requirements and standards of behaviour that apply.

Voluntary staff who are not employees, and students are also under obligations of confidentiality, and must sign an agreement indicating their understanding when helping within the NHS.

Recording patient information accurately and consistently
Maintaining proper records is vital to patient care. If records are inaccurate, future decisions may be wrong and harm the patient. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors.

The information may be needed not only for the immediate treatment of the patient and the audit of that care, but also to support future research that can lead to better treatments in the future. The practical value of privacy enhancing measures and anonymisation techniques will be undermined if the information they are designed to safeguard is unreliable.

Keeping patient information private
This includes aspects such as:

Not gossiping. This is clearly an improper use of confidential information.

Taking care when discussing cases in public places. It may be pertinent to discuss cases with colleagues for professional reasons (to gain advice, or share experience and knowledge), but care must be taken to ensure that others do not overhear these conversations. Generally, there is no need to identify the patient concerned.

Inform Patients Effectively

Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided. Consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then they are not being effectively informed.

In order to inform patients properly, staff must:

- Check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood. These should be available within each NHS organisation;
- Make clear to patients when information is recorded or health records are accessed;
- Make clear to patients when they are or will be disclosing information with others;
- Check that patients are aware of the choices available to them in respect of how their information may be disclosed and used;
- Check that patients have no concerns or queries about how their information is disclosed and used;
- Answer any queries personally or direct the patient to others who can answer their questions or other sources of information;
- Respect the rights of patients and facilitate them in exercising their right to have access to their health records.

Check that patients have seen the available information leaflets

Every NHS organisation should have information leaflets, posters and other materials to support communications about confidentiality and the way that patient information is used and shared.

Must incorporate checks within their everyday working practice e.g.

- Receptionists at clinics or surgeries could ask when patients arrive if they have seen the relevant leaflets, and should offer patients the leaflet if not – this should be supported with encouragement to raise any concerns, perhaps 'Do let me know if you have any queries or would like more information'.
- Clinicians too could check that the patient has had an opportunity to read and understand the leaflets provided – 'Have you read the poster/leaflet on information disclosures and use?'

Make clear to patients when information is recorded or health records are accessed

This may require no more than a comment such as 'Let me note that in your file', or 'I am just taking a note of your blood pressure', and should occur naturally as part of treating patients properly.

Make clear to patients when information is or may be disclosed to others

Patients may know little about how the NHS and related agencies e.g. social services, local government and education work – aspects that staff may take for granted. Staff must ensure that patients know when data is disclosed or used more widely.

Examples might be:

- In respect of a referral letter – 'I am writing to the consultant to let them know about your medical history and the abdominal pains you are having'; or
- With electronic records, 'The hospital specialist is able to view your health records to understand your medical history and the tests we have arranged to date before he examines you'; or
- In respect of other agencies – 'I will tell Social Services about your dietary needs to help them arrange Meals on Wheels for you'.
- There are certain Acts of Parliament that require disclosure – see www.doh.gov.uk/ipu/confiden. Court orders may also require a disclosure. The amount of information disclosed should always be proportionate to the actual need. Even though the patient cannot prevent this disclosure, they must normally be told that it is taking place or that it has already occurred if this is the case.

Check that patients are aware of the choices available in respect of how their information may be used or shared

Patients have the right to choose whether or not to agree to information that they have provided in confidence being used or shared beyond what they understood to be the case when they provided the information. Where the information disclosure hasn't yet taken place, they are also entitled to change their mind.

Check that patients have no concerns or queries about how their information is used

It is important that patients feel free to raise any queries or concerns. In most circumstances it may require no more than a follow-on question to the above: '*Did you understand the leaflet? – Did it make sense to you?*'

In other cases, if it is clear that the information being recorded is particularly sensitive to the patient concerned, staff should be explicit about what information is being recorded, and ask the patient directly if he or she is happy with that information being shared.

Answer any queries personally or direct patients to others who can answer their questions or other sources of information

It is much better for patients if their concerns can be addressed immediately, but, if staff cannot answer the questions properly, they must refer the patient to a better source of information. Most organisations should have arranged back-up contacts for further information e.g. Patient Advisory Liaison (PALs) Officers.

In some areas, e.g. GP surgeries or clinics, procedures may have been set up so that patients' queries can be referred to a local designated individual to avoid disrupting the clinical workload.

Respect the right of patients to have access to their health records

Patients have a right to see and/or have copies of their health records under the General Data Protection Regulation (GDPR)

Communicate effectively with patients to help them understand

It is important to recognise the different communications needs of particular patients. While some may read NHS leaflets when waiting for treatment, others may be disinclined or unable to do so (perhaps through disability, illiteracy, cultural issues or language difficulties). Difficulty in communicating does not remove the obligation to help people understand.

Provide Choice to Patients

Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another – just because something does not appear to be sensitive does not mean that it is not important to an individual patient in his or her particular circumstances.

Staff must:

- Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of, their care;
- Respect patients' decisions to restrict the disclosure or use of information, except where exceptional circumstances apply;
- Communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to or restrict the disclosure of information.

Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of their care.

Where information about patients is required, but does not satisfy the tests of necessity and appropriateness that must govern the use of identifiable patient information, then it should be anonymised to protect the patient.

In all other circumstances efforts must be made to obtain and record consent unless there are statutory grounds for setting confidentiality aside or robust public interest issues.

Respect patients' decisions to restrict the disclosure and/or use of information

In some cases, it may not be possible to restrict information disclosure without compromising care. This would require careful discussion with the patient, but ultimately the patient's choice must be respected.

In the short-term it may not be possible to meet some patients' requests directly though, with some imagination, a compromise arrangement may be possible. This may require discussion about where the patient's concerns really lie as it may be possible to allay those concerns without significant change to the information disclosure arrangements, perhaps by explaining more fully the security arrangements in place, or discussing options in the care process.

It is essential that complete records are kept of all care provided and of any restrictions placed on disclosing by patients. When patients impose constraints it is important to demonstrate that neither patient safety, nor clinical responsibility for healthcare provision, has been neglected.

Explain the implications of disclosing and not disclosing
In order to make valid choices, patients must not only know what their options are, but also what the consequences are of making those choices. Explanations must be proportionate to the risks involved and reflect, where possible, the patient's particular circumstances.

Where patients insist on restricting how information may be used or shared in ways that compromise the health service's ability to provide them with high quality care, this should be documented within the patient's record. It should be made clear to the patient that they are able to change their mind at a later point.

Improve Wherever Possible
It is not possible to achieve best practice overnight.

Staff must:

- Be aware of the issues surrounding confidentiality and seek training or support where uncertain in order to deal with them appropriately.
- Report possible breaches or risk of breaches.

Be aware of the issues surrounding confidentiality, and seek training or support where uncertain in order to deal with them appropriately
Ignorance is no excuse – so staff must be aware of the basic requirements and where support and further information are available and encouraged to seek out training and guidance in order to develop confidential services. Staff must work within both the spirit of this code of practice, and within any locally produced guidelines, protocols and procedures, and be able to demonstrate that they are making every reasonable effort to comply with relevant standards.

Report possible breaches or risk of breach
If staff identify possible breaches or risk of breaches, then they must raise these concerns with their manager or other appropriate colleagues, e.g. the local Information Governance Lead. Staff must be encouraged and supported by management to report organisational systems or procedures that need modification. Staff must be made aware of local procedures for reporting where breaches of confidentiality or abuses of patient data are taking place.

There is specific legislation to protect individuals reporting abuses, as well as NHS procedures to support this where necessary (individual NHS organisations will have their own procedures, or independent advice can be obtained from Public Concern at Work (www.pcaw.co.uk)). Professional staff may also choose to contact their professional, regulatory or indemnifying bodies for specific guidance.

Record Keeping

- Patient records should: be factual, consistent and accurate
- Be written as soon as possible after an event has occurred, providing current information on the care and condition of the patient;
- Be written clearly, legibly and in such a manner that they cannot be erased;

- Be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly;
- Be accurately dated, timed and signed or otherwise identified, with the name of the author being printed alongside the first entry;
- Be readable on any photocopies;
- Be written, wherever applicable, with the involvement of the patient or carer;
- Be clear, unambiguous, (preferably concise) and written in terms that the patient can understand. Abbreviations, if used, should follow common conventions;
- Be consecutive; (for electronic records) use standard coding techniques and protocols;
- Be written so as to be compliant with The Equality Act 2010

Be relevant and useful

- Identify problems that have arisen and the action taken to rectify them;
- Provide evidence of the care planned, the decisions made, the care delivered and the information shared;
- Provide evidence of actions agreed with the patient (including consent to treatment and/or consent to disclose information). And include
- Medical observations: examinations, tests, diagnoses, prognoses, prescriptions and other treatments;
- Relevant disclosures by the patient – pertinent to understanding cause or effecting cure/treatment;
- Facts presented to the patient;
- Correspondence from the patient or other parties.

Patient records should not include

- Unnecessary abbreviations or jargon;
- Meaningless phrases, irrelevant speculation or offensive subjective statements;
- Irrelevant personal opinions regarding the patient.

Threats to Data Security

Keeping patient information physically and electronically secure

This covers both manual and electronic records. Staff should not leave portable computers, medical notes or files in unattended cars or in easily accessible areas. Ideally, store all files and portable equipment under lock and key when not actually being used.

Staff should not normally take patient records home, and where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed.

For all types of records, staff working in offices where records may be seen must:

- Shut/lock doors and cabinets as required.
- Wear building passes/ID if issued.
- Query the status of strangers.

- Know who to tell if anything suspicious or worrying is noted.
- Not tell unauthorised personnel how the security systems operate.
- Not breach security themselves

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the transfer.
- Returned to the filing location as soon as possible after use.
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently.
- Stored closed when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
- Held in secure storage with clear labelling. Protective 'wrappers' indicating sensitivity – though not indicating the reason for sensitivity – and permitted access, and the availability of secure means of destruction, e.g. shredding, are essential.

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished.
- Not leave a terminal unattended and logged-in.
- Not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children's or pet's names or birthdays).
- Always clear the screen of a previous patient's information before seeing another.
- Use a password-protected screen-saver to prevent casual viewing of patient information by others.

Social Engineering

Social engineering is the psychological manipulation of people to steal data or gaining access to information. This can be achieved through many different ways. It could be stealing documentation or devices such as iPad or laptops. Or it could be through a confidence trickster, pretending to be someone else.

Common means of social engineering are:

- **In the office**
  - Someone asking you to hold the door open for them as they have forgotten their key card or slipping in after you.
- **On the phone**
  - A person phoning up pretending to be someone else to gain information.
- **Email**
  - Receiving an email from someone asking for information they are not initiated to or pretending to be someone else to gain the information

    - You may receive an email that when opened allows the sender access to your information
- **Online**
    - Someone tries contacting you or sending a friend request on social media with the purpose of gaining information
    - Someone hacking into your accounts to gain passwords or information
- **Fake IT Department**
    - People may contact you while you are working saying they are from the IT department. They will ask you to your username, password, email address or other details about where you work. They may also try to get you to click on a malicious web or email link.

Steps you can take to prevent Social Engineering:

- When opening an email or message take your time to look at it first, spammers are relying on the fact you will act instantly without checking. Don't open anything you are not sure of and contact your IT department.
- Never give anyone personal details including passwords
- Ensure that your devises have the latest anti-virus and firewall protection
- Check any attachments to email, be cautious before downloading
- Ensure your spam filter is on the highest setting
- Change your passwords regularly and have different ones for each account

Using Social Media Safely

Using social media can leave you venerable to be contacted by people you don't know. This can lead to online bullying or harassment or you inadvertently give personal information to someone you would rather not.

Tips on using Social Media Safely:

- Never disclose private information to anyone when using social media
- Read the site's privacy policy and use its privacy and security settings to control who can see your personal information.
- When picking a user name do not use anything that could identify you
- Use care when accepting inviting friend requests
- Be wary if someone you are contacting with on social media attempts to persuade you to change your beliefs
- Be very careful when clicking on any links
- Use a strong password
- Remember that employers and potential employers frequently view employee's social media page.
- Keep you profile closed, meaning only your friends can view it, not the general public
- Don't post when you are going on holiday or not going to be at home. It advertises your home is empty

Using Email Safely

We rely on using emails regularly for work and home, unfortunately they are used by scammers and spammers. This can lead to annoying adverts or more worryingly identity theft or fraud.

Tips on safe email use:

- Never open emails or click on attachments from unknown senders

- Unsubscribe to any emails you think could be fraudulent
- Type a website address in to the search engine rather than clicking on the link
- Log out when you have finished if on a shared computer
- Change your password regularly and don't let anyone
- Enable filters on your email programs and report spam
- Pay attention to the website's URL

Disclosing Information with Appropriate Care

- **Follow any established information sharing protocols**.

NHS organisations should have developed, or be in the process of developing, information sharing protocols that set out the standards and procedures that should apply when disclosing confidential patient information with other organisations and agencies. Staff must work within these protocols where they exist, and within the spirit of this code of practice where they are absent.

- **Identify enquirers, so that information is only shared with the right people.**

Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information.

- **Ensure that appropriate standards are applied in respect of e-mails, faxes and surface mail**

Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be. Guidance is available on the Department of Health web-site at www.doh.gov.uk/ipu/confiden.

- **Share the minimum necessary to provide safe care or satisfy other purposes.**

This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties), and is likely to constitute a breach of confidence. The Caldicott principles should be followed.

Confidentiality: NHS Code of Practice provides advice on patient confidentiality issues, and states: "Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information."

Inevitably, there are occasions when professionals and staff disclose personal confidential information by mistake. Such mistakes can result in serious consequences.
In addition to reporting any such breach to managers, it is imperative that the safety of the patient whose confidence has been breached is uppermost in everyone's mind and appropriate advice is sought as soon as the error has been detected. Expert advice can be sought from:

- Professional regulators;
- National standards and statements;
- Organisational policies;
- Caldicott Guardians and information governance specialists;
- Professional insurers; and
- Line managers.

The Deceased

There is a lack of consistency in the approach to the data of deceased people within the health and social care system. The common law duty of confidence is generally regarded as extending to the deceased but the General Data Protection Regulation (GDPR) only relates to the living. Legal representatives or those with a claim on the estate of a deceased person are able to access the health records of the deceased person through the Access to Health Records Act 1990, but there is no equivalent legal route for access to social care records. Some 'work-arounds' are used but these are increasingly untenable.

As people gain more control of their information, it should be possible for a person to give custodianship of their personal confidential data after their death to someone, or to a research data bank, so that future generations can use it to learn and improve the health and wellbeing of society.

The review panel concluded that the Law Commission, in their review of the legal aspects of data sharing should consider looking at how the law surrounding deceased persons might be better harmonised. In particular, the Panel would like the Law Commission to consider ensuring there are no legal impediments to giving custodianship of their health and social care data within their last will and testament.

The NHS Constitution

The Review Panel proposes that alongside giving due regard to consent, professionals and staff within health and social care should adhere to the rights, pledges and duties set out in the NHS Constitution.

The Review Panel recommends that these rights, pledges and duties be extended to include the whole health and social care system, which includes but is not limited to the NHS, public health, researchers and local authorities. If it was extended in that way, it would read as follows:

- You have the **right** of access to your own records and to have any factual inaccuracies corrected.
- You have the **right** to privacy and confidentiality and to expect the health and social care system to keep your confidential information safe and secure.
- You have the **right** to be informed about how your information is used.

- You have the **right** to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

Using and Disclosing Confidential Patient Information

The disclosure and use of confidential patient information needs to be both lawful and ethical. Whilst law and ethics in this area are largely in step, the law provides a minimum standard that does not always reflect the appropriate ethical standards that the government and the professional regulatory bodies require.

For example, the Department of Health and the General Medical Council are in agreement that, whilst there are no clear legal obligations of confidentiality that apply to the deceased, there is an ethical basis for requiring that confidentiality obligations, as outlined in this document, must continue to apply. Further, where the law is unclear, a standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

Legal Considerations There are a range of statutory provisions that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. Generally, however, there are four main areas of law which constrain the use and disclosure of confidential personal health information.

Common Law of Confidentiality This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Whilst judgements have established that confidentiality can be breached 'in the public interest', these have centred on case-by-case consideration of exceptional circumstances. Confidentiality can also be overridden or set aside by legislation.

The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018. (Taken from the Information Commissioners Office).

The GDPR applies to 'Personal Data', this means any data that can directly or indirectly identify a person. Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

Human Rights Act 1998 (HRA98) Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records.

Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:

- Pursue a legitimate aim;
- Be considered necessary in a democratic society; and
- Be proportionate to the need.

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need.

Administrative Law Administrative law governs the actions of public authorities. According to well-established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e. beyond its lawful powers. It is also necessary that the power be exercised for the purpose for which it was created or be "reasonably incidental" to the defined purpose. It is important that all NHS bodies be aware of the extent and limitations of their powers and act "intra vires"

The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the ultra vires rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, e.g. by obtaining explicit patient consent.

Consent Issues

Competence to Consent

Seeking consent may be difficult, either because patients' disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty communicating their decision (be it to consent or object).

In the former case, extra care must be taken to ensure that information is provided in a suitable format or language that is accessible (e.g. providing large print or Braille versions of leaflets for those with reading difficulties) and to check that it has been understood.

In the latter case, it will be important to check for a clear and unambiguous signal of what is desired by the patient, and to confirm that the interpretation of that signal is correct by repeating back the apparent choice.

Failure to support those with disabilities could be an offence under the Equality Act 2010, and may prevent consent from being gained. Support for communicating with patients having specific disabilities can be obtained from a range of agencies.

Children and Young People

Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also

entitled to make decisions about the use and disclosure of information they have provided in confidence (e.g. they may be receiving treatment or counselling about which they do not want their parents to know).

However, where a competent young person or child is refusing treatment for a life threatening condition, the duty of care would require confidentiality to be breached to the extent of informing those with parental responsibility for the child who might then be able to provide the necessary consent to the treatment.

In other cases, consent should be sought from a person with parental responsibility if such a person is available. It is important to check that persons have proper authority (as parents or guardians). Ideally, there should be notes within the child's file as to any unusual arrangements.

Where patients are unable to give consent

If a patient is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the health professionals concerned must take decisions about the use of information. This needs to take into account the patient's best interests and any previously expressed wishes, and be informed by the views of relatives or carers as to the likely wishes of the patient. If a patient has made his or her preferences about information disclosures known in advance, this should be respected.

Sometimes it may not be practicable to locate or contact an individual to gain consent. If this is well evidenced and documented and anonymised data is not suitable, the threshold for disclosure in the public interest may be lessened where the likelihood of detriment to the individual concerned is minimal. Where explicit consent cannot be gained and the public interest does not justify breaching confidentiality, then support would be needed under Section 60 of the Health and Social Care Act 2001.

Where the patient is incapacitated and unable to consent, information should only be disclosed in the patient's best interests, and then only as much information as is needed to support their care.

This might, however, cause unnecessary suffering to the patient's relatives, which could in turn cause distress to the patient when he or she later learned of the situation. Each situation must be judged on its merits, and great care taken to avoid breaching confidentiality or creating difficulties for the patient. Decisions to disclose and the justification for disclosing should be noted in the patient's records. Focusing on the future and care needs rather than past records will normally help avoid inappropriate disclosures.

Such circumstances will usually arise when a patient has been unable to give informed consent to treatment, and, provided the patient has not objected, this may justify the disclosure of some information with relatives in order to better understand the patient's likely wishes. There may also be occasions where information needs to be shared with carers in order to assess the impact of disclosures to the patient him or herself. Such occasions are rare and justifiable only in the best interests of the patient.

Patients are often asked to indicate the person they would like to be involved in decisions about their care should they become incapacitated. This will normally, but not always, be the 'next of kin'. It should be made clear that limited information will be shared with that person, provided the patient does not object. This gives patients the opportunity to agree to disclosures or to choose to limit disclosure, if they so wish.

Explicit Consent

When seeking explicit consent from patients, the approach must be to provide:

- Honest, clear, objective information about information uses and their choices – this information may be multi-layered, allowing patients to seek as much detail as they require;
- An opportunity for patients to talk to someone they can trust and of whom they can ask questions;
- Reasonable time (and privacy) to reach decisions;
- Support and explanations about any form that they may be required to sign;
- A choice as to whether to be contacted in the future about further uses, and how such contacts should be made; and
- Evidence that consent has been given, either by noting this within a patient's health record or by including a consent form signed by the patient.

The information provided must cover:

- A basic explanation of what information is recorded and why, and what further uses may be made of it;
- A description of the benefits that may result from the proposed use or disclosure of the information;
- How the information and its future uses will be protected and assured, including how long the information is likely to be retained, and under what circumstances it will be destroyed;
- Any outcomes, implications, or risks, if consent is withheld (this must be honest, clear, and objective – it must not be or appear to be coercive in any way); and
- An explanation that any consent can be withdrawn in the future (including any difficulties in withdrawing information that has already been shared).

The information provided must allow for disabilities, illiteracy, diverse cultural conditions and language differences.

The Right to Withhold or Withdraw Consent

Patients do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment.

There are a number of things to consider if this circumstance arises:

- The concerns of the patient must be clearly established and attempts made to establish whether there is a technical or procedural way of satisfying the concerns without unduly compromising care.
- The options for providing an alternative form of care or to provide care through alternative arrangements must be explored.
- Decisions about the options that might be offered to the patient have to balance the risks, staff time and other costs attached to each alternative that might be offered against the risk to the patient of not providing healthcare.

Every effort must be made to find a satisfactory solution. The development of technical measures that support patient choice is a key element of work to determine the standards for electronic integrated care records. Careful documentation of the decision making process and the choices made by the patient must be included within the patient's record.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018. There are additional rules in the GDPR for organisations processing special category data. This includes information about an individual's health. (Taken from the Information Commissioner's Office).

Personal data is defined in the GDPR as:
"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The GDPR covers the processing of personal data in two ways:

1. Any personal data that is processed wholly or partly in electronic form
2. Any personal data that is processed which forms part of, or is intended to form part of a filing system

If the Personal Data is of a more sensitive nature it will require a higher level of protection. The GDPR refer to this as 'special categories of personal data'.

This includes:

- Race
- Ethnic Origin
- Political Opinions

- Regions or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sex life or sexual orientation

Personal data can include information relating to criminal convictions and offences.

Data Protection Principles

Article 5 of the GDPR require that Personal Data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals
2. Collected for specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes: further processing for archiving purposes in the public interest, specific or historical research purposes or statistical purposes shall not be considered to be compatible with the initial purpose;
3. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;
4. Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archive purposes or statistical purposes subject to implementation of the appropriate technical and organisation measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR introduces a duty for public authorities to appoint a Data Protection Officer (DPO). A DPO must be independent, an expert in data protection and adequately resourced. The DPO assists with monitoring internal compliance, advising on data protection obligations, providing advice on Data Protection Impact Assessment and act as a contact point.

Freedom of Information Act 2000

What are the principles behind the Freedom of Information Act?

The main principle behind freedom of information legislation is that people have a right to know about the activities of public authorities, unless there is a good reason for them not to.

This means that:

- Everybody has a right to access official information. Disclosure of information should be the default – in other words, information should be kept private only when there is a good reason and it is permitted by the Act
- An applicant (requester) does not need to give you a reason for wanting the information. On the contrary, you must justify refusing them information
- Requests for information must be treated equally, except under some circumstances relating to vexatious requests and personal data. The information someone can get under the Act should not be affected by who they are. You should treat all requesters equally, whether they are journalists, local residents, public authority employees, or foreign researchers
- Because all requesters should be treated equally, you should only disclose information under the Act if you would disclose it to anyone else who asked. In other words, you should consider any information you release under the Act as if it were being released to the world at large.

Organisations you can ask for information

You can request information from some public sector organisations, e.g.:

- Government departments, and other public bodies and committees
- Local councils
- Schools, colleges and universities
- Health trusts, hospitals and doctors' surgeries
- Publicly owned companies
- Publicly funded museums
- The police

How to make an FOI request

Contact an organisation in writing to make a Freedom of Information (FOI) request. This can be by:

- Letter
- Email
- Fax

What to include
You should give:

- Your name (not needed if requesting environmental information)
- A contact address
- A detailed description of the information you want - eg you might want all information held on a subject, or just a summary

You can ask for information in a particular format, e.g.:

- Paper or electronic copies of information
- Audio format
- Large print

Alternatively…
A request must be in writing and can be either posted or emailed to NHS England.

For postal requests, please send to the following address:
NHS England
PO Box 16738
Redditch
B97 9PT

Email requests should be sent to **england.contactus@nhs.net**

Write “Freedom of Information” in the subject line.

When you’ll get a response
You should get the information within 20 working days. The organisation will tell you when to expect the information if they need more time.

Costs
Most requests are free but you might be asked to pay a small amount for photocopies or postage. You’ll be told by the organisation if you have to pay anything.

The Confidentiality Model

The model outlines the requirements that must be met in order to provide patients with a confidential service. Record holders must inform patients of the intended use of their information, give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be ongoing to aid the improvement of a confidential service.

The four main requirements are:

PROTECT – look after the patient's information;

INFORM – ensure that patients are aware of how their information is used;

PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways. To support these three requirements, there is a fourth:

IMPROVE – always look for better ways to protect, inform, and provide choice.

Glossary

Patient identifiable Information

Key identifiable information includes:

- Patient's name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients;
- NHS number and local patient identifiable codes;
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

Anonymised Information

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.

Psyeudonymised Information

This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However, it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.

Explicit or Expressed Consent
This means articulated patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

Implied consent
This means patient agreement that has been signalled by behaviour of an informed patient.

Healthcare Purposes
These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.

Information Sharing Protocols
Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security, confidentiality and data destruction, between two or more organisations or agencies.

Medical Purpose
Medical purposes include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001 explicitly broadened the definition to include social care.

Public Interest
Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.

References

Confidentiality: NHS Code of Practice
Information Security Management: NHS Code of Practice
Record keeping Guidance for nurses and midwives
Records Management:
NHS Code of Practice Part 1
Records Management NHS Code of Practice Part 2 (2nd Edition)
The NHS Constitution – the NHS belongs to us all
ICO Information Commissioner's Office - GDPR

