HEALTHWATCH ENGLAND

Information Security & Governance Policy

Version:	1
Name of organisation / author:	Simon Richardson /Gerard Crofton-Martin
Date issued:	Nov 2016
Review date:	Nov 2017
Target audience:	All Healthwatch England Staff

The following handbook is a summarised version of the CQC **Information Security and Governance Policy** produced for Healthwatch England use.

1. Introduction

i. What is information governance

Information Governance is the system of controls (policies, processes, systems etc.) by which an organisation ensures that it meets its legal, policy and moral obligations in relation to the processing of information.

ii. Importance of information governance

Healthwatch England holds and has access to sensitive information, such as; information about people who use services, care providers and our own staff; commercially sensitive information about care providers; and information from CQC and strategic partners about regulatory activity and other actions to protect people from harm and improve the quality of services.

Loss, misuse or mishandling of this information creates a direct risk to the privacy, dignity, rights and welfare of people who use services and may significantly damage the effectiveness of Healthwatch and CQC.

It is particularly important to maintain public trust in the confidentiality and security of their personal information within the wider health and social care system. Loss of this trust may significantly impact upon the effectiveness of the health and social care sectors.

iii. Information Governance Framework and key roles

CQC has an **Information Governance Group** which includes Healthwatch England representation.

The group is chaired by CQC's **Senior Information Risk Owner** (SIRO) (the Board member with delegated responsibility for ensuring that information risks are appropriately managed) and **Caldicott Guardian** (the senior manager with responsibility for ensuring that information about people who use services is appropriately handled and used).

The Information Governance Group report directly to the CQC Executive Team and the Audit and Corporate Governance Committee. They have delegated responsibility for decision making on matters of information management, information security, information risk management, legal compliance with information law, information sharing and the organisation's statutory responsibilities under the Freedom of Information Act 2000, the Data Protection Act 1998, and other relevant legislation.

2. Confidentiality

i. Importance of confidentiality

Some information held by Healthwatch England carries the risk of adverse or damaging effects if disclosed.

Most obviously, private information about individual people carries the risk of affecting their privacy, dignity, safety or welfare if disclosed. The handling of this type of information is covered in section 5 of this handbook.

However, it is important to remember that other types of information may be confidential in nature too. For example, releasing information about a care provider may have a significant commercial impact upon their business. Information about planned or ongoing regulatory activity could prejudice the effectiveness of that activity. Information about government policy development or the management of CQC or Healthwatch England may pre-empt official announcements with damaging effect.

Whenever handling information, you should be mindful of whether the information is confidential in nature. Where appropriate, confidential information should be marked as such, and should always be handled with care.

We are still able to collect, use and share confidential information, but we should only do so with appropriate consideration, and where we are satisfied that our actions are lawful and in the public interest.

ii. Legal requirements

In some cases, Healthwatch England will be covered by legal requirements of confidentiality. Our legal responsibility to protect information about people is covered in section 5, but there are also specific prohibitions on publishing information about ongoing CQC enforcement activity and on disclosures of commercially sensitive information obtained by CQC as part of the adult social care 'market oversight' role. If information of this type has been shared with Healthwatch England colleagues by other parts of CQC, these legal prohibitions on disclosure still apply.

In any case, where Healthwatch has received information of a confidential nature (i.e. where disclosure has the potential to cause some damage or harm) in circumstances where it is reasonable to expect that we would protect that confidentiality (whether or not this has been explicitly agreed), we will be subject to the common law duty of confidentiality.

Whether there is a specific prohibition on disclosure or where the general common law duty of confidentiality applies, we may still have a legal basis to disclose information – but we must still exercise care in protecting the

information and making these decisions. This is covered further in section 6 of this handbook.

3. Knowledge and Information Management

i. Importance of records management

Records provide vital evidence of business decisions, activities and transactions. They are also essential in ensuring that Healthwatch England (HWE) meets legislative and regulatory requirements.

Healthwatch England has access to training and guidance to ensure staff understand their legal responsibilities and can apply best practice in managing records. The key benefits for supporting Healthwatch England in this are that records are:

- Captured and stored in the right place.
- Authentic so are confident that records are accurate.
- Accessible in a timely way, by those who need or have a right to see them.
- Protected from unauthorised deletion, changes or access.
- Disposed of appropriately once they are no longer required.

Primary records should be held in electronic format to meet the requirements of the government's digital strategy and to support easy access. Therefore the policies and associated guidance that support records management are designed to achieve this goal and to also support the management of records that only exist in paper format.

ii. Naming convention

Records must be named consistently to make them easier to find and so that, if needed, they can be moved between systems efficiently without causing conflicts or data loss. The naming convention policy defines the:

- Content and structure of file names
- Characters that must not be used
- Methods of ensuring files can be located and versions identified
- Appropriate use of protective markings

When you; create a new electronic file, update an existing file, or need to store a file you have received, you should name it in accordance with the file naming convention.

Our naming convention has five components as follows:

1. Date (formatted as YYYYMMDD)
2. Name
3. Record type
4. Version (if applicable)
5. Protective marking (if applicable, that is use for OFFICIAL SENSITIVE files)
   If the information is OFFICIAL there is no need to indicate this in the naming convention.

An example of the naming convention is as below:

20150401 CQC Board Meeting minutes v1

Our naming convention is restricted to alphanumeric entries (i.e. no special symbols or characters), with each of the components being separated by a space only.

Specifically the following characters are forbidden from our naming convention as they can cause conflicts with other systems and software used within CQC and HWE:

> < : " * ? \ / | ~ _ + = , . ; ' ^ !) (& % £ $ # @

iii. Storage of records

Our policies and guidance support record storage and maintenance by defining standards for:

- Protecting sensitive or confidential information.
- Sharing records.
- Version control.
- Storing and maintaining paper.
- Managing records within shared systems.

P: Drives should only be used to store personal work-related files and should not be used to store Healthwatch England records or documents on a permanent basis. Short-term temporary storage of documents or copies of records is allowed for use when offline but should be removed as soon as network connection is available.

E-mail

Each member of staff is assigned a limited personal mailbox allowance to ensure that Outlook is not used as the primary storage location for Healthwatch England records.

All records required for business purposes must be held in a central location to ensure that they remain accessible. Therefore, email records must be transferred to HWE's agreed repository as soon as possible and not stored in Outlook or in P: Drives for longer than necessary.

iv. Retention of records

All records used, received or created by Healthwatch England must have a retention period assigned that meets legislative and business requirements. Once this period ends, records must be either transferred for permanent storage or destroyed in a way appropriate to their content and storage format. This applies to all records whether electronic or physical (such as paper records). The government's Digital Strategy says that records should be held in electronic systems therefore the use and storage of paper records should be minimal.

Retention periods are included in the Information Asset Register. The IAR also identifies the record owners, the sensitivity of the information they contain and their format and location.

Records that are no longer required must be destroyed securely as soon as possible in an authorised and systematic way as described in the disposal process.

v. **Information asset ownership and management**

CQC has an information Asset Management responsibility structure in place for managing our information which reflects UK government best practice. The structure is also followed within Healthwatch England in partnership with CQC. Information Assets are those which are listed in the Information Asset Register. There are four levels of role to the structure, Senior Information Risk Owner (SIRO), Information Asset Owner (IAO), Information Asset Manager (IAM) and KIM Champion. The roles are filled as additional responsibilities by staff at CQC and Healthwatch. For further information about these roles, please email RDM.Helpdesk@cqc.org.uk.

vi. **Accessing records**

For general access to HWE's electronic storage structures, new staff members need to complete the mandatory Knowledge and Information Management level 1 training.

For access to restricted areas staff must obtain authorisation from the Information Asset Owner, Team Manager (for the relevant area) or KIM champion.

Whether restricted or not, you must only access Healthwatch England records as authorised and required for the exercise of your role.

When a staff member changes teams, the RDM.Helpdesk@cqc.org.uk should be notified to remove them from the team access groups. When a staff member leaves the organisation their account is disabled and shortly after it is deleted.

4. **Information Security**
   - i. Importance of Information Security
   - ii. Key information security requirements
   - iii. Protective marking
   - iv. Identifying and reporting information security incidents

5. **Using personal data and confidential personal information**

i. **What is personal data**

Personal data is defined under section 1 of the Data Protection Act 1998, it is information that relates to and identifies a living person, either on its own or

when combined with other information we hold (or which is likely to come into our possession).

Some personal data - such as information about a person's ethnicity, religion, sexuality or sexual life, trade union membership, physical or mental health, or about alleged offences or prosecution – is defined as 'sensitive personal data' and is subject to greater legal protection.

ii. What is confidential personal information

Confidential personal information is defined under section 76 of the Health and Social Care Act 2008. It is personal data that has been obtained by CQC (including by Healthwatch England) in circumstances requiring it to be held in confidence.

This could mean that there was an explicit agreement of confidentiality when information was provided to Healthwatch, or that a reasonable person would have considered that a duty of confidentiality was implied.

iii. Legal requirements and obligations

The Data Protection Act provides a set of Principles that must be followed when 'processing' (holding, obtaining, handling, using, sharing, altering, disposing of) personal data. The Health and Social Care Act 2008 creates a specific offence of disclosing confidential personal information except in defined circumstances.

<u>Fair processing</u>

The most fundamental requirement of Data Protection compliance is 'fair processing'. A key element of fair processing is a 'no surprises' approach where people are informed of who has their personal data, how they will use it and why. Processing someone's personal data in a way that would be a surprise to a reasonable person is unlikely to be fair, and would therefore be unlawful.

This creates an obligation to tell people, at the point where you collect their information, how and why you will use it. If there are elements of your intended use that are optional, the person should be told this and given an easy way to exercise choice. Where personal data is being collected via a third party, reasonable steps should be taken to communicate this information back to the 'data subject'.

<u>Lawful processing</u>

Processing of personal data must also be 'lawful'. This requires that all of the Data Protection Principles must be met, the rights of individuals under the Act (e.g. the right to see what information we hold about them, to correct inaccurate information, and the right to object to the processing of information

in ways which are damaging to them) must be complied with, and we must process personal data in accordance with other laws (such as the Human Rights Act 1998, which requires that any intrusion upon personal privacy must be justified and proportionate).

Conditions for processing personal data

Personal data may only be processed where a condition under schedule 2 of the DPA is met.

Sensitive personal data (information about a person's racial or ethnic origin, political opinions, religious (or similar) beliefs, trade union membership, physical or mental health, sexual life, or relating to offences, alleged offences or prosecution) may only be processed where a condition under schedule 3 of the DPA is *also* met.

Schedule 2 conditions that are likely to apply to the processing of personal data by Healthwatch England are:

Condition 1: Consent of the data subject,
Condition 4: Necessary to protect the vital (life or death) interests of the data subject,
Condition 5: Necessary for the administration of justice, the exercise of statutory functions, or for the exercise of functions of a public nature.
Condition 6: Necessary for 'legitimate' (e.g. lawful and reasonable) interests being pursued by the party disclosing, or by the party receiving, the personal data – except where the disclosure would be unwarranted by reason of prejudice to the rights, freedoms or legitimate interests of the data subject.

Schedule 3 conditions that are likely to apply to the processing of sensitive personal data by Healthwatch England are:

Condition 1: Explicit consent of the data subject
Condition 2: Necessary for compliance with, or for exercising rights under, employment law
Condition 3: Necessary for protecting the vital interests of the data subject, or any other person, in a case where consent cannot be given or where it would not be reasonable to seek consent.
Condition 5: The personal data has previously been made public as a result of steps deliberately taken by the data subject
Condition 6: Necessary for the purpose, or in connection with legal proceedings or for the purpose of obtaining legal advice

Condition 7: Necessary for the administration of justice, or the exercise of statutory functions

Condition 8: Necessary for "medical purposes" (including the management of healthcare services) where the person sharing and the person receiving the information owes a duty of confidentiality equivalent to those of a health professional. [Note: CQC's position is that the offence of disclosure of confidential personal information, under section 76 of the Health and Social Care Act 2008, which applies to all CQC and NGO employees, establishes this equivalent duty]

There are also additional regulations which create the following schedule 3 condition permitting disclosure of sensitive personal data:

Regulation 2: The disclosure is in the substantial public interest and necessary for the discharge of functions designed to protect the public from dishonesty, malpractice, serious improper conduct, or the unfitness or incompetence if any person where it must necessarily be carried out without explicit consent of the data subject being sought so as to prevent prejudice to the discharge of that function.

iv. Necessity Test

The necessity test is the decision making process designed to assist in reaching lawful decisions on obtaining, using and sharing confidential personal information/data.

The person considering the disclosure should understand what 'legitimate purpose' they are seeking to achieve by the proposed disclosure (e.g. which function of Healthwatch England, or CQC, or other outcome in the public interest they are trying to achieve).

They should satisfy themselves that the intended action will be fair and meet a schedule 2 (and, for sensitive personal data, also a schedule 3) condition (see above). Then they should consider the two-step test:

STEP 1: Is the disclosure a necessary step in achieving this outcome?

If the outcome could reasonably be achieved, in an efficient and effective manner and within the available resources, by other means, then personal data should not be shared. For example, could anonymised or aggregated data be used instead?

This step should include consideration of whether the minimum personal data required to achieve the purpose is being shared. We should not share more personal data than necessary.

STEP 2: Is the proposed disclosure proportionate?

Consideration should be given here to the likely impact upon the privacy and interests of the data subject (including any objections they have raised) and these should be balanced against the anticipated public interest to be served by disclosure.

In short, having considered the necessity test, the person should be satisfied that they would be able to explain and justify their actions if challenged.

v. Anonymisation and pseudonymisation

Wherever possible, anonymised or pseudonomised data should be used instead of personal data / confidential personal information. Data of this type can be more freely used or shared, and its use minimises the risk to the privacy and dignity of individuals.

Anonymised data is information from which it is not possible to identify individuals – for example, aggregated data showing statistical information about large numbers of people.

Pseudonymised data is information where the identities of individuals are concealed, but where re-identification is possible – for example, narrative information about a person's care where their name is replaced with a pseudonym such as 'patient A'.

Care should be taken as simply removing names, addresses etc. does not always guarantee that individuals cannot be identified.

Full guidance on anonymisation and pseudonymisation is available here [link] and advice should be sought if in doubt.

vi. Authorisation to use PD/CPI – PIA, Caldicott and SIRO

When considering new ways of using information – for example, planning the introduction of new systems, processes or policies – consideration should be given as to whether the proposed changes will involve changes to the way in which personal data or other confidential information will be obtained, used, stored or shared. Where this is likely to be the case, appropriate authorisation must be sought.

Privacy impact assessments are a structured way to assess the likely risks to personal privacy arising from changes, and for putting appropriate measures in place to mitigate those risks. Where the proposed changes will involve information about people who use care services, the privacy impact assessment will form part of the Caldicott approval process.

The Caldicott Guardian's role is to ensure that uses of information about people who use services are lawful, fair and proportionate.

Privacy impact assessments, and any other changes to the processing of confidential information, must be signed off by the Senior Information Risk Owner (SIRO). The SIRO's role is to ensure that all information risks have been identified and are being properly managed.

6. Information Sharing

i. Why we share information

The appropriate and effective sharing of information can play a vital role in protecting people from harm, improving services and in facilitating the exercise of Healthwatch, CQC and strategic partners.

ii. Legal requirements

Personal data must only be shared where it is fair and lawful to do so.

Consideration should be given to whether data subjects would reasonably have expected their personal data to be shared by Healthwatch. In making this assessment, consideration should be given to any information previously provided to the data subject, any discussions with them, any indication they have given about how they wish or expect their data to be used, and publicly available information materials about uses of information.

Consideration may also be given to what information the data subject themselves has put into the public domain. Where they have made their own information public, then it is more likely to be fair to share that information – however, care should be taken in differentiating between information that the person has made public and information that they may reasonably expect to be maintained in confidence.

Where it is considered that the data subject would not reasonably expect their information to be shared, they should be contacted and their consent sought for the disclosure.

Where it is not appropriate or possible to do this, consideration should be given to whether there is another lawful basis which would permit a disclosure which would otherwise be unfair. The only exemptions which are likely to apply are:

- Where the disclosure is necessary for the prevention or detection of crime, or the prosecution of offenders. This may apply where the disclosure is considered to be necessary for regulators to investigate allegations of serious breaches of regulations or offences relating to registered activities.

- Disclosures which are necessary in connection with legal proceedings, proposed legal proceedings, or for the purpose of obtaining legal advice.

In other cases, exceptional circumstances may permit the sharing of information. Most notably, a disclosure that is considered necessary to protect a person from significant risk of serious harm would be permissible.

iii. Making decisions to share information

Decisions on sharing personal data should be made using the 'necessity test' (see section 5(iv)). Confidential medical information about identifiable people should only be shared without consent where there is a very high public interest in doing so.

Decisions on sharing other kinds of information should take into account the potential impact of disclosure and the possible prejudice or damage that may be caused.

iv. Authorisation

You should only share information if you are authorised to do so as part of your role, or where you have authorisation to do so from the information asset owner or an appropriate senior manager.

v. Sharing information with other parts of CQC

Decisions on sharing information with other parts of CQC should be made on the same basis as sharing with external bodies.

7. Access to Information

i. Into to FOIA, EIR and DPA SARs

Healthwatch England, as part of CQC, has a statutory responsibility to respond to requests for information made under various legislation.

Section 7 of the Data Protection Act gives data subjects a right of access to information Healthwatch England holds about them. This is called a subject access request (SAR).

The Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations (EIR) give a general public right of access to any information held by Healthwatch England – subject to some exemptions.

SARs must be answered within 40 days. FOIA and EIR requests must be responded to within 20 working days.

The CQC Information Access Team handles SARs, FOIA and EIR requests on behalf of Healthwatch England.

ii. What to do if you receive a request

If you receive a written request for information – even if it does not mention DPA, FOIA and EIR – and if you are not confident that you can handle it in the normal course of business, or if you consider that we may want to refuse the request or withhold some information, you must forward it to information.access@cqc.org.uk immediately.

iii. What to do if asked to support a request

The Information Access Team may request your help in handling a request for information. You may be asked to locate and extract requested information, or to provide advice on the background of the information or potential impact of disclosure (to help consider possible exemptions).

It is important to provide the requested assistance in a timely manner to help ensure compliance with these statutory requirements.

iv. Sign-off and decision making

All responses to requests for information from Healthwatch England are signed off by the Healthwatch England Chief Executive (or a nominated senior manager). Sign off may be escalated to the CQC Chief Executive where the Information Access Team cannot reach agreement on a disclosure with the Healthwatch England Chief executive.

v. Disclosure of information about you

As a public employee, you should be aware that information about your role, professional decisions and actions may be disclosed in response to requests. Generally speaking, information of a personal nature will not be disclosed.

The more senior and public facing your role, the more likely it is that information about you may have to be disclosed. Where potentially sensitive or confidential information about you is being considered for disclosure, you will be consulted.

8. Support and guidance

i. Who to come to for advice/assistance

- Deputy Director – Neil Tester
- Strategy Planning and Performance Manager – Sandra Abraham

ii. Guidance and policies

Full guidance on information governance issues can be found here.

FAQs

1. **Who is the Senior Information Risk Owner (SIRO)?**

The current SIRO is Malte Gerholt, CQC's Executive Director of Strategy & Intelligence.

2. **Who is the Caldicott Guardian?**

The current Caldicott Guardian is Professor Sir Mike Richards, Chief Inspector of Hospitals.

3. **What is the difference between the role of Caldicott Guardian and the Senior Information Risk Owner (SIRO) role?**

The Caldicott Guardian's role is to ensure that information about people who use health and social care services is used, handled and shared appropriately. They give advice and guidance and consider proposals for uses of patient and service-user information by assessing compliance with the Caldicott Principles (see below).

The SIRO's role is to provide assurance to the Board that information risk (see below) is being properly managed.

The SIRO is supported by Information Asset Owners (IAO's) who have responsibility for specific parts of the information we hold (for example, an 'information asset' such as a database or collection of records) and who provide assurance to the SIRO that these are being properly protected and managed.

4. **What are the Caldicott Principles?**

The Caldicott Principles are a set of rules that should be followed by all organisations that handle 'patient identifiable information' (information which identifies, or could be used to identify, people who use health or social care services):

- **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.

- **Don't use patient identifiable information unless it is 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).

- **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.

- **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.

- **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.

- **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.

- **The duty to share information can be as important as the duty to protect patient confidentiality**
  Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.

5. What is 'information risk'?

Information Risk is the term applied to any risk arising from the obtaining, use, storage, transfer, handling, disclosure or disposal of information.

It includes 'information security risks' – risk that information may be lost, damaged, corrupted or accessed by unauthorised persons – but is wider than this. For example, we have recognised information risks that we may not be transparent and open in how we work, that we may fail to properly use the information we hold to exercise our functions, or that we may retain and store information for longer than we need it.

6. Who is the Information Asset Owner (IAO) in HWE?

The IAO in Healthwatch England is Neil Tester, Deputy Director.

7. What Information Governance Training do I need to complete?

All Healthwatch England staff need to complete 'Knowledge and Information Management – Level 1' when they join the organisation, and 'CQC Values and Information' when they join and every year.

8. What's the difference between a record, document and asset?

Documents are information stored in any format, such as blank forms, reference books, leaflets or posters.

Records are documents that contain evidence of business activity created or collected in the course of that activity – for example emails, spreadsheets, databases, photographs or audio recordings.

An information asset is a body or collection of information that we define as a single unit so that it can be understood and managed effectively. For example, we may define a database, or a collection of paper records, or a collected set of folders on the Y: drive as information assets.

9. What do I do if I receive an FOIA, EIR and DPA SARs request?

If you receive a request for information that you would not usually provide as part of your usual role, please pass the request to information.access@cqc.org.uk as quickly as possible – we only have 20 working days to respond.

If you are asked to assist the Information Access Team by locating or providing information, or by advising them on issues relating to information they are considering for disclosure, please do so as fully and quickly as possible to help them meet this legal obligation.

10. What is an information security incident?

An information security incident is an event where information held by (or on behalf of) Healthwatch England is; lost, destroyed, corrupted, compromised or accessed by unauthorised persons, or where it is processed unlawfully, or where we have a 'near-miss' where such an outcome is narrowly averted.

Examples of information security incidents include:

- Confidential information being sent to the wrong person
- Confidential paper records being disposed of in normal waste, or stolen from an employee's home or vehicle
- An unauthorised person getting access to an Healthwatch England systems or data on an unencrypted device
- A computer virus infecting an Healthwatch England systems and corrupting data
- A poorly written survey resulting in the unplanned collection of sensitive personal data

11. How do I report an Information security incident?

If you become aware of an incident involving information security you must report it immediately to your line manager, the HEALTHWATCH ENGLANDIAO (see above) and to security@cqc.org.uk

This will allow any necessary steps to be taken to limit the incident, and to ensure that any lessons are learned.

When reporting an incident, explain what has happened, when and how, and any steps you have taken but do not include confidential personal information in the initial report.

12. What is a Privacy Impact Assessment (PIA)?

A PIA is a defined process by which we seek to understand the likely impact of our intended actions on people's privacy. The assessment includes consideration of the risks to privacy and of steps that we can take to mitigate these.

A PIA should be conducted whenever we are considering a change to our systems or processes that has any significant potential to interfere with privacy. The PIA should be conducted early in the project and returned to and updated regularly.

13. What is Information Sharing?

Information sharing is – quite simply – the sharing of information between various organisations.

Appropriate information sharing is vital to the effective delivery of health and social care services, and sharing information with regulators, commissioners and a range of other strategic partners plays a key role in the effective oversight of the health and social care sectors. We may also share information with the police and safeguarding partners to help identify and tackle abuse and other crimes.

However, it is vital that we share information in ways that is lawful and ethical, and that confidential information – especially personal information – is only shared where it is necessary and proportionate to do so.

CQC has produced guidance on information sharing, and the Information Access Team can provide advice and assistance.

14. What is anonymisation?

Anonymisation is any process to reduce the likelihood that any individual can be identified from any set of information or data.

Data is considered to be anonymised once it reaches a level where the likelihood of any individual being identified from it is sufficiently remote that there is no reasonable likelihood of re-identification.

There are various techniques for achieving anonymization – for example by 'aggregating' information so as to create statistical information about a large number of people, or by 'redacting' (deleting or editing out) specific information that could be used to identify them.

The extent to which we need to go to anonymise data will depend upon the sensitivity of that data and the level of risk associated with re-identification. For example, we may need to take significant steps to anonymise information about whistle-blowers, or information about people's health conditions.

CQC has produced guidance on anonymization – http://intranetplus.cqc.local/Directorates%20Teams/Customer%20Corporate%20Services/Governance%20Legal%20Services/Governance/Information%20Rights/Documents/Anonymisation%20Guidance.pdf

15. What is pseudonymisation?

Pseudonymisation is a specific anonymization technique whereby information that could directly identify a person (for example, their name 'Margaret Smith') is replaced with a substitute (for example, 'Patient A').

This can be a useful technique for anonymization, but should be used with care.

Pseudonymisation can be reversed by anyone who obtains the 'key' to the information (for example, a separate list saying who Patients A, B, C and D are).

Also, pseudonymised information is still focussed on the individual, so it is often possible for people to be identified from it. For example, if the information shows that Patient A is an Asian woman, aged 57, from Islington, with skin cancer, it starts to become reasonably likely that some people may be able to identify her. Increasingly, social media and online search tools are presenting a risk to individuals being re-identified from pseudonymised information.