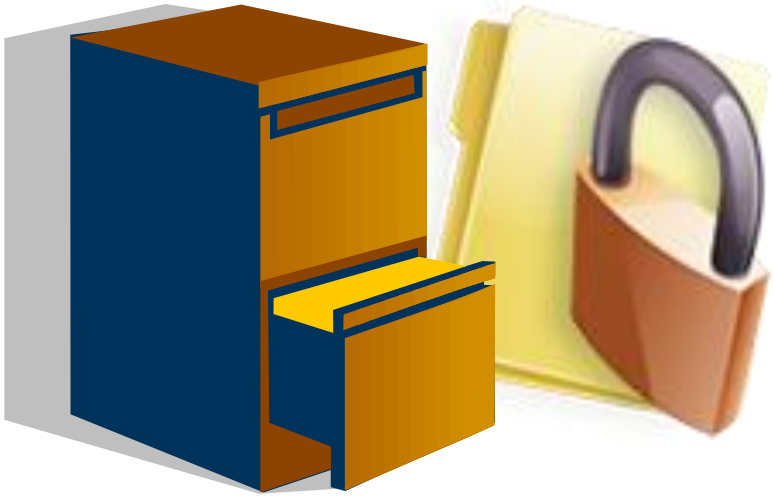
Somerset Community Health

INFORMATION GOVERNANCE TRAINING

WORKBOOK AND QUIZ



Name:

Date:

Annual Refresher Due:

July 2011

INFORMATION GOVERNANCE

The NHS uses the term ‘Information Governance’ to describe the rules on handling information. This term covers issues such as Data Quality (making sure information is accurate and available), Records Management (a systematic method of recording information), Data Protection (which places obligations on how personal information is used) and confidentiality and security. Confidentiality and security measures overlap and support each other. Information Governance covers all information – confidential and non-confidential – across the Trust.

The NHS holds 'Personal and Sensitive Personal Information' about millions of people – NHS staff as well as our patients.

The details are names, addresses, dates of birth, NHS numbers AND related information about physical or mental health condition.

Safeguarding such a large amount of this information in a lockable area such as a Patient Records Department (or an HR Department) is fairly secure - but information is not obtained simply to store in locked rooms. The information is required wherever it is needed – on wards, clinics, sent and received by departments across a Trust, between Trusts or other healthcare providers and letters are sent to patients that contain their confidential health information.

Information can be split into 4 types:

Confidential – private information about you; given to somebody who has a duty of confidence (i.e., healthcare professional); you expect it to be used in confidence – UK law says that health information is confidential

Personal – all information about a person (name, address, loyalty card details, car you drive, where you went to school, etc) – UK law sets out rules which must be followed by any organisation collecting or using personal information

Sensitive Personal – racial or ethnic origin, political opinions, religious belief, union membership, physical or mental health condition, sexual life, criminal record – UK law says that health information is sensitive personal. Other sensitive personal information includes that which could cause damage/distress, i.e. bank/passport details

Anonymous – NHS number, reference number - if information is lost, it is unlikely that person can be identified. Think – could a patient with a rare illness be identified because of that?

WHAT MUST BE PROTECTED?

Confidential information

Common law cases show that a person can take legal action if their confidentiality is broken – this may be by disclosing information to others or failing to protect the information. This covers personal information which a patient gives to the NHS (e.g. name and address) - and sensitive personal information (e.g. health details).

Personal information

UK law says that personal information must be protected by adequate security e.g.: our names, addresses and dates of birth are held by government when we register to vote – and these details must be protected by adequate security.

Sensitive personal information

The same applies to sensitive personal information (the information must be protected by adequate security). The law recognises that the damage or distress caused by a loss or misuse of your sensitive personal information may cause greater damage or distress – which implies even greater protection measures are needed than that required for personal information. It also covers non-health information (e.g. criminal record or ethnic background, sexual orientation) of a job applicant or member of staff who discloses this information to their employer.

WHY PROTECT IT?

Legal Obligations and Penalties

UK laws demand that we protect these types of information. A person can take legal action if their confidentiality is broken – and a court can decide the amount of compensation to be paid. From April 2010 organisations are liable to a fine of up to £500,000 for reckless use of personal information.

And of course there are other reasons:

Providing a Confidential Service

We provide a confidential health service – which is a promise made to the public (set out in the NHS Constitution and Patient Guarantee)

Patient Trust

If patients don't trust us with their information, then how can we provide quality care without reliable records – or even contact our patients?

WHAT INFORMATION DOES NOT REQUIRE PROTECTION?

Anonymous information - 'anonymous' means the person cannot be identified – and therefore this is neither personal nor confidential – so does not require protection for the purposes of maintaining confidentiality (though there may be other reasons why this should be protected e.g. if it is copyrighted or commercially valuable).
Personal and Sensitive Personal Information in the Public Domain - there are times when personal and sensitive personal information is publicly available and there can be no expectation of confidentiality e.g.:

- newspapers publish the names and address of people convicted of speeding and other crimes; political and religious figures are photographed and named

- names of senior management and other appointments which are publicly accountable – Chief Executives, Directors, Heads of Medical Services

- members of the public, patients or staff who willingly take part in publicity material and give consent for their name and photograph to be used

- members of the public, patients or staff who take part in publicly accountable forums such as Public Board Meetings

- staff in public facing roles – such as nurses and receptionists who deal face to face with members of the public

- names of NHS managers and staff who write letters to patients – we cannot send un-named, unsigned letters

In each of these cases the information disclosed should be limited to what is required e.g. of names on a badge or identity card - not additional information which is not justified.

CONFIDENTIALITY MEASURES

The duty of confidence regulates the sharing of (disclosure) written and spoken information - but information needs to be shared with other staff needing the information to provide a patient with effective healthcare. So how do we comply with the duty of confidence – yet make sure we provide high quality care?

We implement Confidentiality Measures - which allow information to be shared - but only under strict controls to ensure the duty of confidence is maintained. These measures include:

Restricting people - who can have access to the information e.g. the Doctor disclosing information only to those who need it – such as a consultant to whom the patient is referred or staff that need to type a letter or issue repeat prescriptions.

Restricting information - restricting the information that these people can have i.e. providing only the information that is needed for them to do their job – no more and no less – such as staff performing administrative work may need to access patient addresses but not their clinical details.

Training Staff - making sure all employed staff understand their duty of confidence, the confidentiality measures and their responsibilities.

Enforcing - contract clauses – adding confidentiality obligations and disciplinary clauses in employment contracts for all staff AND adding confidentiality obligations and penalties in service contracts with external organisations (such as IT Engineers, window cleaners) who might come into contact with information.

These measures are aimed at everyone who might see or overhear confidential information – cleaners, messengers, maintenance staff, IT staff, volunteers, porters, caretakers, drivers, catering and laundry staff.

SECURITY MEASURES

Security Measures protect against risks to the organisation – including risks such as loss, theft or compromise of the information we need to protect. The measures can be grouped into three types:

- physical measures
- people measures
- electronic measures

WHO SHOULD PROTECT INFORMATION?

The Board

The senior management level of the organisation (e.g. a Board or a senior partner in a GP Practice) is ultimately responsible for the organisation's compliance with all legal obligations – which include the appropriate use and protection of personal information.

Health Professionals and all employees

UK law allows health information to be used for medical purposes if it is used by a health professional, or a person who owes an equivalent duty of confidentiality. So we can only provide medical (health) services if we meet this requirement – hence each organisation must include confidentiality (and security) obligations in the terms and conditions of employment and job descriptions - so we all have an enforceable obligation (these measures are also applied to temporary staff, honorary workers, volunteers, contractors and anyone else who may come into contact with information who is employed by the organisation or may be given access to information for which the organisation is responsible).

WHEN SHOULD INFORMATION BE PROTECTED?

It should be protected from the time it is created to the time it is destroyed (securely e.g. by shredding or incineration). This means 24 hours a day, 7 days a week wherever the information is located:

Locations

In offices, in briefcases, on trains, in clinics, on wards and whatever format it is in:

Formats

- Digital (e.g. e-mail, patient admin systems)
- Hard copy (e.g. patient letters, appointment books, medical notes, X-rays, test results)

The Duty of Confidence

The duty of confidentiality remains with staff after employment with the NHS ends – to ensure that information obtained during our NHS employment remains confidential.

Information Technology

General Advice

- In public rooms or rooms to which the public may have access, terminals or screens should be placed facing away from the normal access routes.

- Staff should use a password-protected screensaver, lock their workstation or log off if there is someone present who is not authorised to view information.

Passwords

The use of passwords is the primary method of ensuring data security. There is sometimes a temptation to share passwords or to display them on notes attached to the side of the screen. These and similar practices severely compromise security measures. To ensure that unauthorised access to Trust systems is prevented, passwords must be kept private.

Internet Access

The internet link is provided for Trust authorised business. Reasonable personal use is permitted provided this does not interfere with the performance of work duties. A Line Manager can limit personal access to the internet and staff must act in accordance with the guidelines of their Line Manager. The Trust takes no direct responsibility for the actions of any individual with regard to the misuse of the internet.

Email

The e-mail system is provided for Trust authorised business and the Trust takes no direct responsibility for the actions of any individual with regards to misuse of the e-mail system.

Due to the insecure nature of internet mail, users must consider e-mail and other information to be public information. Staff should bear in mind that all information produced can be made publicly available under the Freedom of Information Act if it is requested. Staff should not consider information sent or received through the e-mail system as their private information.

Only the following methods are acceptable for emailing patient identifiable information:

- email between users on the same email server. The Trust uses a range of email servers and email between users on somerset.nhs.uk is secure as is

somcomhealth.nhs.uk and also e-mails sent to somerset.gov.uk (Social Services/Education Department) from Somerset.nhs.uk or somcomheath.nhs.uk email addresses

- using NHSmail (www.nhs.net) at both the sending and receiving end (i.e., from @nhs.net email address to @nhs.net email address). Note that email from @somerset.nhs.uk to @nhs.net and vice versa is NOT secure and should not be used unless suitably encrypted before sending.

- encrypting an email attachment to NHS standards (SecureSend).

Use of Facebook and other Social Media

NMC Guidelines

The code (Standards of conduct, performance and ethics for nurses and midwives) states that nurses and midwives must "uphold the reputation of your profession at all times" (NMC 2008), while students must "uphold the reputation of your chosen profession at all times" (NMC 2009a). This means that conduct online and conduct in the real world should be judged in the same way, and should be at a similar high standard. Nurses and midwives will put their registration at risk, and students may jeopardise their ability to join the register, if they:

- share confidential information online
- post inappropriate comments about colleagues or patients
- use social networking sites to bully or intimidate colleagues
- use social networking sites in any way which is unlawful

This list is not intended to be exhaustive. If there is any doubt about whether a particular activity online is acceptable, it can be useful to think through a real-world analogy. For example, manipulated photos that are intended to mock individuals would be considered offensive if printed and pinned on workplace notice boards, and are no less offensive when shared online, even when privately shared between friends.

Royal College of Nursing Guidance

Here are some critical do's and don'ts to remember:

- don't make disparaging remarks about your organisation, its clients or fellow employees on a social network site
- avoid any identification of your employer on your profile page of a social network site
- don't make any remarks on a social network site that may embarrass your employing organisation. In particular, do not air your grievances where countless others might be able to read all about it
- don't use the social networking site or other non-work related sites when you are supposed to be working
- under no circumstances identify patients in your care, or post information that may lead to the identification of a patient. If you do, you interfere with their

privacy and breach the law on confidentiality, your employment contract and your professional Code of Practice
- never post sexually explicit, racially offensive, homophobic or other unlawfully discriminatory remarks on your network site
- read and comply with your employer's policy on IT use in the workplace

Social Networking – Assessing the Risks – All Staff

Any form of online posting can expose you to risk. Message boards and blogs are both considered to be public mediums and material posted on those resources is subject to the same laws as those for print. The best advice is to avoid making comments about your employer and/or work colleagues/management. A few words posted on your blog, Facebook page or message board could be read by numerous people.

Use of Laptops

Users of laptops must ensure that all sensitive files are password protected (note that these passwords cannot be recovered if lost/forgotten), disks and paper copies containing valuable software or sensitive data must be locked away in briefcases or containers when in transit and particular care should be given to the security of laptops when in transit. They must be securely locked and not left on general view.

Laptops must not contain any patient identifiable information – use an encrypted memory stick and any user taking any equipment home should check that their household insurance covers loss, theft and damage.

Operate a Clear Screen Policy

When you leave your computer remember to press 'Ctrl' + 'Alt' + 'Delete' and lock your computer so that it cannot be accessed by anybody who is not authorised. Your computer can only be accessed by using your user name and password and you must not share your password with anyone else.

Operate a Clear C Drive Policy

No data, confidential or not, should be stored on the 'C' drive of a computer.

USB/Memory Sticks

Thousands of USB sticks are lost or stolen each year causing personal, sensitive and confidential data to be lost or, more worryingly, exposed. The Information Commissioner, who monitors how we follow the Data Protection Act principles, has been granted the ability to impose higher fines for those who breach any of the rules.

Our Trust policy allows ONLY the use of Trust Approved password protected sticks. Speak to your Line Manager if you need one.

WHAT IS THE FREEDOM OF INFORMATION ACT?

This Act gives the public a right of access to any files or information held by the Trust. There are some exemptions but the general rule is that we have to provide

the information unless we can show there is a good, public interest, reason not to. If a request is turned down, the applicant has a right of appeal to the Information Commissioner, who is appointed by Parliament to ensure that the Act is complied with.

Anybody can make a request under the act – this includes commercial companies, journalists, patients and the public. They have the right to ask for the information they want and there is no need for them to tell us why they want it.

The Act applies to any information held by the Trust, in any form – electronic as well as paper records. If your files contain scraps of paper with rough notes you have made or comments, then these are just as disclosable as "official" letters and memos. Emails have to be treated in the same way. You should write everything, including emails, in a way you would not mind them being read by members of the public and the press.

The Act is fully retrospective, which means that it applies to all information, including that created prior to the Act coming into force. It does not apply to requests to see personal data, including health records, which are covered by the Data Protection Act 1998 and the Access to Health Records Act 1990 (if the request is to see the health records of a deceased patient).

Freedom of Information requests have to be made in writing – an email counts as a written request. We have a maximum of 20 working days to confirm whether or not we have the information requested and to provide it.

WHAT IS THE DATA PROTECTION ACT?

The Data Protection Act 1998 became law in March 2000. It sets standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. These are summarised by 8 Data Protection Principles. As well as information held on computers, the Data Protection Act 1998 also covers most manual records e.g.

- Health
- Finance
- Personnel
- Suppliers
- Occupational Health
- Contractors
- Volunteers
- Card Indices

THE 8 DATA PROTECTION PRINCIPLES

Personal data must be:

1 Processed fairly and lawfully

2 Processed for specified purposes

3 Adequate, relevant and not excessive

4 Accurate and kept up-to-date

5 Not kept for longer than necessary

6 Processed in accordance with the rights of data subjects

7 Protected by appropriate security (practical and organisational)

8 Not transferred outside the EEA without adequate protection

PRINCIPLE 1 - Processed fairly and lawfully

There should be no surprises, so ... inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with e.g.

- when formulating a research project remember to be open and transparent about what you will be doing with the information
- when working in a team, ensure that the patient/client is aware of who the members of the team are, and that all those involved with their care may need to see their notes
- be open, honest and clear

PRINCIPLE 2 - Processed only for specified purposes

Only use personal information for the purpose(s) for which it was obtained e.g.

- personal information on a Patient Administration System must only be used for healthcare purposes - not for looking up friends' addresses or birthdays
- only share information outside your practice, team, home, ward, department or service if you are certain it is appropriate and necessary to do so
- if in doubt, check first!

PRINCIPLE 3 - Adequate, relevant and not excessive

Only collect and keep the information you require. It is not acceptable to hold information unless you have a view as to how it will be used. Do not collect information "just in case it might be useful one day!" e.g.

- taking both daytime and evening telephone numbers if you know you will only call in the day
- explain all abbreviations
- use clear legible writing
- stick to the facts - avoid personal opinions and comments

PRINCIPLE 4 - Accurate and kept up-to-date

Take care when inputting information to ensure accuracy. How do you know the information is up-to-date? What mechanisms do you have for checking the Information is accurate and up-to-date? e.g.

- each time a patient attends a clinic, they should be asked to confirm that their details are correct - address, telephone number etc.
- check existing records thoroughly
- before creating new records
- avoid creating duplicate records

PRINCIPLE 5 - Not kept for longer than necessary

Follow retention guidelines for the record (HSC 1999/053) GP records (HSC 1998/217)

- check the Trust's Records Management Strategy and Guidelines
- ensure regular housekeeping/spring cleaning of your information
- do not keep "just in case it might be useful one day!"
- check the organisation's disposal policy
- dispose of your information correctly

PRINCIPLE 6 - Processed in accordance with the rights of data subjects

- subject access requests
- confidentiality
- prevent processing for direct marketing - an end to junk mail and faxes!
- automated decision taking
- compensation

- rectification/blocking/erasure
- request an assessment

PRINCIPLE 7 - (Practical)

Protected by appropriate security

- ensure security of confidential faxes by using Safe Haven/Secure faxes
- ALWAYS keep confidential papers locked away
- do you have a clear desk policy?
- ensure confidential conversations cannot be overheard
- keep your password secret
- ensure information is transported securely

PRINCIPLE 7 - (Organisational)

Protected by appropriate security your organisation should have ...

- good information management practices
- guidelines on IT security
- staff training
- confidentiality clause in employment contracts
- procedure for access to personal data
- a disposal policy/procedure for confidential information
- confidentiality contracts with third parties e.g.
    - archiving companies
    - cleaners
    - temporary staff
    - outside contractors

PRINCIPLE 8 - Not transferred outside the European Economic Area (EEA) without adequate protection

- if sending personal information outside the EEA ensure consent is obtained and it is adequately protected
- be careful about putting personal information on websites - gain consent first
- check where your information is going e.g.

The EEA comprises: United Kingdom, France, Belgium, Germany, Denmark, Ireland, Netherlands, Sweden, Portugal, Spain, Finland,

To sum up, remember that information must be:

- held securely and confidentially
- obtained fairly and efficiently
- used effectively and ethically
- recorded accurately and reliably
- shared appropriately and lawful

WHAT IS CALDICOTT?

The term Caldicott refers to a review commissioned by the Chief Medical Officer. A review committee, under the chairmanship of Dame Fiona Caldicott, investigated ways in which patient information is used in the NHS.

The review committee made a number of recommendations aimed at improving the way the NHS handles and protects patient information. These are summarised by six Information Management Principles.

The Six Caldicott Principles

1 Justify the purpose(s) of using confidential information

2 Only use it when absolutely necessary

3 Use the minimum that is required

4 Access should be on a strict need-to-know basis

5 Everyone must understand his or her responsibilities

6 Understand and comply with the law

RECORDS MANAGEMENT

We all have a responsibility to ensure that the single largest activity, that of obtaining, storing, disseminating and transferring or destroying information across the trust, complies with Acts/Regulations

Almost all NHS information held and used by the Trust comes under the Department of Health Code of Practice – Records Management
Records should be healthy when CURED!

- **C**reating: Good quality records - are they accurate? Up to date? Complete (including NHS Number or other reference)? Easy to find? Free from duplication? Not disjointed?

- **U**sing: Within Acts and Regulations

- **R**etention: Safe storage and archive in line with NHS recommended retention schedule

- **E**valuate: Are the records worthy of permanent archive?

- **D**isposal: Appropriately according to policy

Best practice guidance states:

All staff have a legal and professional obligation to be responsible for any records which they create or use in the performance of their duties.

Any record created by an individual, up to the end of its retention period, is a public record and subject to information requests (FOI and DPA)

LAW AND GUIDANCE – further reading

- Data Protection Act 1998

- Freedom of Information Act 2000

- Information Security Standards – ISO/IEC 17799:2005 and IS Management NHS Code of Practice

- The NHS Confidentially Code of Practice

- The Records Management NHS Code of Practice

- Information Quality Assurance

- The Human Rights Act 1998 (Article 8)

- The Public Records Act 1958

- Common Law Confidentiality

- The NHS Care Record Guarantee

LOCAL POLICY AND PROCEDURES/GUIDANCE

- Data Quality Policy
- Records Management Strategy
- Records Keeping Standards
- Information Management Technology Strategy
- Data Protection Policy
- Freedom of Information Policy
- Information Governance Systems Security Policy and Procedures
- Whistle-blowing Policy

INFORMATION GOVERNANCE TEST

1 The Information Governance Lead is at a photocopier and finds a pay statement left in the machine. It is a hospital employee's. What should he do with this?

a ☐ Leave it on the photocopier and hope the person comes back to collect it

b ☐ Tell his line manager and suggest sending the statement to the Pay Department and reporting the incident

c ☐ Go and look for the person and hand it to them

d ☐ Rip it into shreds and put it into a bin

2 The Information Governance Lead is working at his computer when he receives an unexpected email. He sees that it contains a list of patients that are receiving dialysis treatment. What should he do with the email?

a ☐ Delete it

b ☐ Delete it but also mention it to his line manager when convenient

c ☐ Forward the e-mail to colleague and ask what to do

d ☐ Tell his line manager, report the incident and secure the information

3 The Information Governance Lead's manager is going through a completed job application forms sent from HR. The ethnicity sections of the form have **not** been removed before being sent to her. She asks him if this is okay. What should he say?

a ☐ Tell his manager that it's fine - as long as she treats the information confidentially

b ☐ Tell her that this is confidential 'sensitive personal' information which should be securely returned to the HR and reported

c ☐ Tell her that it is 'sensitive personal' information but nothing to worry about

d ☐ Tell her that she should call HR and complain

4 The Information Governance Lead's workmate phones him; he says that he is moving some empty cabinets and has just found a full HR file stuck at the back of one of them. What should his workmate do?

a ☐ Put the file in an office waste bin and move the cabinet

b ☐ Put the file in the internal mail to the HR Dept

c ☐ Have a quick look through it and leave it in the cabinet

d ☐ Tell his line manager, suggesting the file should be returned to HR and the incident reported

5 The Information Governance Lead finds a sheet of paper on the floor of a hospital corridor. It is a leaflet showing opening times for the staff shop. On the back is written a name, address and telephone number. It is not a name he knows and it is not a hospital telephone number. What should he do?

a ☐ Ring the number and tell whoever answers that a sheet has been found with these details on

b ☐ Rip the personal details into small bits and throw them in the bin

c. ☐ Pin the leaflet to a nearby notice board where it might be found

d ☐ Put the sheet of paper in his pocket and think about it later

6 The Information Governance Lead is sitting on the bus home. Someone who knows him is sitting nearby and asks him what the hospital visiting times are because her uncle was admitted to the hospital that morning. What can he say?

a ☐ Tell his friend the visiting times

b ☐ Tell his friend that he cannot say as this is confidential information

c ☐ Tell his friend that he cannot say as this is personal information

d ☐ Tell his friend that he cannot say as this is sensitive personal information

Which <u>Principle</u> does each scenario or breach relate to? (There may be more than one)

7 Mr Smith receives a call from the local hospital to tell him that his pregnant wife has been admitted. He is very shocked, as they have been divorced for 10 years and his ex-wife re-married his best friend. Mr Smith informed the hospital that he is no longer her next of kin

_____

_____

_____

_____

8 A Mother asks to see her 16 year old daughter's School Nurse reports as she suspects her daughter is sexually active. The School Nurse says no problem, asks for the request to be in writing and says she will provide a copy of recent notes within 21 working Days

_____

_____

_____

_____

9 A health records assistant has been tasked with checking 100 random health records to see whether they are labelled with the correct NHS Number. She decides that there is not enough space in her department to do this task comfortably, so she finds a quiet meeting room in the Post Graduate Centre to do this. She pops out for lunch for an hour leaving the notes unattended and room unlocked

_____

_____

_____

_____

10 Mrs Jones moves from London to Leeds and registers herself with a new GP in Leeds. The GP goes through her records to get familiar with his new Patient's health history. He finds abbreviations such as HT and NLW in the notes. When he contacts the previous GP to explain – he laughs and says oh that means 'Hot Totty' and 'Nice Looking Woman'.

_____

_____

_____

_____

11 A Nurse is approached by PC Bloggs asking how his Brother (also a Police Officer) is doing after having been shot in the line of duty. Nurse mentions that he is stable in terms of the gun wound, but they have found that his cancer has spread. When the Brother regained consciousness he was surprised to find that his Brother (PC Bloggs) knew about the cancer. Only his wife knew until now.

_____

_____

_____

_____

12 HR were approached by the their Trusts communications team asking for all staff home addresses to do a mail shot regarding the benefits for staff and training opportunities available when the implementation of the new National Programme for IT is complete at their Trust. HR agreed to email the staff database to the communications team as soon as possible.

_____

_____

_____

_____

13 A USA Social Services team heard that a UK Social Care team were using new and successful techniques to handle manic depressive young teenagers. The USA team ask for a report on the methodology supported by real life case reports so that they can learn from UK findings. The UK Team send case notes and reports via email to the USA team.

_____

_____

_____

_____

14 A Finance Assistant is tasked with disposing of any old requisitions filed. Her colleague tells her to get rid of any cleared requisitions which are more than 18 months old. The assistant found 50+ requisitions which were nearly 3 years old which exceeds the recommended retention period in the DH Records Management NHS: Code of Practice.

_____

_____

_____

_____

15 A famous celebrity is taken ill while performing at a local theatre. Appendicitis is diagnosed and the celebrity requires emergency surgery. The anaesthetic practitioner recognises the celebrity and following the surgery rings a friend to tell them about this surgery and other information of this celebrity's past healthcare history. The following day a newspaper publishes details of the surgery and other health issues the celebrity has.

_____

_____

_____

_____

16 How many days do you have to reply to a Freedom of Information request?

a ☐ 20 days

b ☐ 40 working days, including weekends

c ☐ 20 working days

d ☐ 2 years

17 Who can make the decision as to whether to disclose health information?

a ☐ anybody

b ☐ the patient

c ☐ one lead qualified clinical person

d ☐ the Chief Operating Officer

18 Give examples of 4 pieces of PERSONAL information

_____

_____

_____

_____

19 Which of the following passwords would be accepted as secure?

a ☐ password

b ☐ my cats name

c ☐ date of birth2011

d ☐ Db98765!

20 What is Information Governance?

_____

_____