Information Governance (IG)

Checklist

- Read through this section of the workbook
- Complete the on-line assessment via the intranet (see 'e-learning quick start guide' – pages 1 – 4) for details on how to access this
- If further information is required please contact the Information Governance Team on ext. 1240

What is IG?

- IG is to do with how **NHS & Social Care** organisations and their employees **handle information**
- IG is a series of **best practice** guidelines and principles of the **Law** to be followed by NHS & Social Care organisations and their employees
- IG is the core foundation for high **quality healthcare** using good **quality information**
- IG applies to **all types and formats of information** and data handled by the Trust
- IG is the responsibility of **every employee** and is a **contractual obligation**

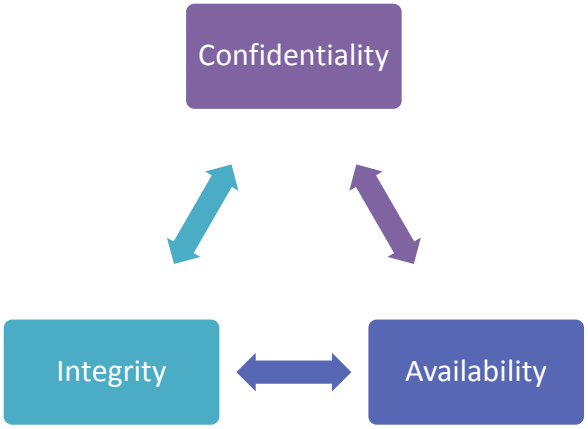
Types of information
Personal data: *Information that identifies a person (on its own or when combined with other information) e.g. name, date of birth, home address, NHS number, hospital number, staff number etc.* ***An unusual name or unique post code can be sufficient to identify a person on their own.*** ***Sensitive personal data:*** *e.g. religious beliefs, ethnic origin, criminal record, medical records etc.* ***Confidential information:*** *Information given in confidence and which is owed a duty of confidence e.g. information disclosed by patients to healthcare staff; employee references; some commercial information about the Trust* ***Corporate data:*** *Information relating to the running of the hospital e.g. Trust accounts; statistical reports; contracts; minutes of meetings etc.* ***Pseudonymised information:*** *Information in which an individual's identity is disguised by using a unique identifier (a pseudonym) that does not reveal their 'real world' identity, but allows the linking of different data sets for the individual concerned.* ***Anonymised data:*** *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 may lead to identification.* ***Anonymised data does not identify a person, so it cannot be personal or confidential.***
Formats
Paper records; electronic records; electronic databases; audio recordings; video records; CDs; DVDs; photographs; x-rays, emails, text messages etc.

Why IG is important

IG aims to ensure the creation of high quality information, in a secure working environment, in order to provide better quality healthcare to patients.

Confidentiality underpins the bond between the Trust and its patients and serious data or confidentiality breaches can put the Trust and its staff in the media spotlight which can damage the organisation's reputation, lead to a loss of confidence and possible enforcement action.

Data security is central to confidentiality and maintenance of good information to support patient safety (Safe Data, Safe Care). Data security can be broken down into three areas – ***Confidentiality, Integrity and Availability***:



Confidentiality *– is about privacy and ensuring that information is only accessible to those with a proven need to see it*

Integrity *– information is protected against loss or damage and can be relied on (it is correct and un-modified)*

Availability *– information is available when and where it's needed to support care*

Confidentiality

Confidentiality is a legal obligation that is derived from case law, known as the ***common law duty of confidentiality***, and is a requirement established within professional codes of conduct and NHS employment contracts.

Failure to meet the standards set out in the Confidentiality clause of Trust employment contracts can result in disciplinary action, termination of a contract, dismissal and in some cases criminal charges.

Information that individuals disclose in confidence **should not** be used or shared further without a lawful reason i.e.:-

- with consent of the individual
- there is a legal reason to disclose
- there is a public interest justification.

Decisions to disclose without consent should be made by senior staff. In LHCH this is our IG Manager or Caldicott Guardian.

Informing people

Patients and service users will not expect health and care professionals to look at their record unless they are involved in their care. You should inform patients and service users that you are accessing and using their information. There are specific techniques you should use when doing so:

Explain	Give choice
Clearly explain to people how you will use their personal information and point them to additional information about this. Information is available on our website and in our leaflet 'In Confidence: Protecting your privacy'	Give people a choice about how their information is used and tell them whether that choice will affect the services offered to them.
Meet expectations Only use personal information in ways that people would reasonably expect.	

You don't need to obtain consent every time you use or share personal information for the same purpose, providing you have previously informed the individual – they should know what is happening and have no objections.

Confidentiality - sharing information for care

Sharing information with the right people can be just as important as not disclosing to the wrong person. Where sharing will assist the care or treatment of an individual – and it is reasonable to believe that they understand the information sharing that is needed to support that care – you have a duty to share the information (***The Health and Social Care (Safety and Quality) Act 2015***).

Check	Best practices
Check that the individual understands what information will be shared and has no concerns.	Ensure that the data protection, record keeping and security best practices covered later in this workbook are met.
Respect objections Normally, if the individual objects to any proposed information sharing, you must respect their objection even if it undermines or prevents care provision. Seek guidance from our IG Team or Caldicott Guardian	

Confidentiality – sharing for non-care

Information that can identify individual patients **must not** be used or disclosed for purposes other than their direct healthcare **without** the individual's explicit consent, this includes medical research.

If however there is a risk of immediate harm to the patient or to someone else you should discuss the request with the Information Governance Team or Caldicott Guardian. Information should **only** be released when authorised.

If you are unable to discuss with the Information Governance Team or Caldicott Guardian then you should share the information and then contact the Information Governance Team as soon as possible afterwards.

Implied consent *– patient agreement has been signalled by behaviour of an informed patient.*

Explicit consent *- articulated patient agreement i.e. a clear and voluntary indication of preference or choice that is freely given in circumstances where the available options and the consequences have been made clear. Documented consent is preferable to ensure auditability*

Competence to consent *– Consent is only valid when the patient understands what they are agreeing to, so care must be taken to ensure patients fully understand and have enough time to agree, or object, to what is being suggested or asked*

The Caldicott Principles for using & disclosing patient information

Always follow the seven Caldicott Principles before using or disclosing confidential patient-identifiable information for a non-healthcare purpose without patient consent, and **never** disclose if you are unsure about any of your responses to the Caldicott principles / questions.

Follow the requirements set out in Information Sharing Agreements, were these have been established to govern routine sharing of personal information with other organisations.

Principle 1: Do you have a justified purpose for using this confidential information?
The purpose for using confidential information should be justified, which means making sure there is a valid reason for using it to carry out that particular purpose

Principle 2: Are you using it because it is absolutely necessary to do so?
The use of confidential information must be absolutely necessary to carry out the stated purpose.

Principle 3: Are you using the minimum information required?
If it is necessary to use confidential information, it should include only the minimum that's needed to carry out the purpose.

Principle 4: Are you allowing access to this information on a strict need-to-know basis only?
Before confidential information is accessed, a quick assessment should be made to determine whether it is actually needed for the stated purpose. If the intention is to share the information, it should only be shared with those who need it to carry out their role.

Principle 5: Do you understand your responsibility and duty to the subject with regards to keeping their information secure and confidential?
Everyone should understand their responsibility for protecting information, and recipients of information must also be made aware of their own responsibility for protecting the information they receive and must be informed of the restrictions on further sharing.

Principle 6: Do you understand the law and are you complying with the law before handling the confidential information?
There are a range of legal obligations to consider when using confidential information. The key ones that must be complied with by law are provided by the common law duty of confidentiality and under the Data Protection Act 1998. If you have a query around the disclosure of medical or other confidential personal information you should go to your Line Manager initially, then the IG Team if you are still not sure. For serious and complex issues contact the IG Team who will contact our Caldicott Guardian for advice and guidance.

Principle 7: Do you understand that the duty to share information can be as important as the duty to protect confidentiality?
You should have the confidence to share information in the best interests of your patients and service users within the framework set out by these principles. Additional local support and guidance is available on our intranet, in our policies and from the IG Team.

If you are not sure, DON'T DISCLOSE, seek further advice from your Line Manager, the IG team or Caldicott Guardian

Patients' right to confidentiality

It is the duty and commitment of the NHS to keep patients' health information safe, secure and confidential. Patients have a right to privacy and confidentiality and to expect the NHS to keep their confidential information safe and secure, whether that information is in electronic or paper form. Regulatory bodies have also made it clear that they too expect the NHS to put in place the strongest safeguards available.

To maintain privacy and confidentiality, it is a requirement that electronic record systems only permit those who have a genuine 'need to know' to access a patient's information, and then only where it is reasonable to believe that the patient concerned would not object, or he/she has been asked for permission.

Electronic Patient Records (EPR)

While EPR delivers numerous benefits over paper-based case notes it also provides greater access to patient data, therefore records **must only** be accessed where a **legitimate relationship** exists.

The system is fully auditable and any inappropriate access identified will be investigated and could lead to disciplinary action being taken including dismissal.

A 'legitimate relationship' means the member of staff is working in a team involved in the patient's care. Any member of staff accessing a patient's clinical information must have a legitimate relationship with the patient.

A legitimate relationship with the patient will be when the EPR record has been accessed by a registered and regulated health professional who is involved in the direct care of the patient and when any or all of the following criteria are met:

- The individual presents themselves to the professional to receive care
- The individual agrees to a referral from one care professional to another
- The individual is invited by a professional to take part in a screening programme for which they are eligible and they accept
- The individual presents to a health or social care professional in an emergency situation where consent is not possible
- The relationship is part of a legal duty
- The individual is told of a proposed communication and does not object e.g. Consultant states they will contact another professional for opinion and the patient does not object

Non-clinical members of staff **must only** access the EPR where they have a **legitimate business reason** to access the patient's clinical information as part of their job role for example members of the clinical audit team.

Data Protection

The ***Data Protection Act 1998*** governs how personal data belonging to living individuals is processed and incorporates eight principles of good information handling.

The principles give people specific rights in relation to their personal data and put certain obligations on the organisations that are responsible for processing it.

The Act applies to computerised information and to structured manual records.

The most relevant rights in healthcare setting are:

- the right to be informed about what their personal information is being used for and who it may be shared with (known as ***fair processing***)
- the right to see and have a copy of their information (known as ***subject access***)

Data Protection Principles
1. Fair and lawful
2. Purposes
3. Adequacy
4. Accuracy
5. Retention
6. Rights
7. Secure
8. International

- the right to have objections to the processing of their information be considered where the individual claims they're suffering unwarranted distress or damage as a result

The main obligations placed on the Trust are:

- to only use personal information for the purpose for which it was obtained and to only collect the information needed for that purpose
- to ensure information is accurate & update and not kept longer than needed
- to keep personal data secure, taking appropriate security measures to prevent data being accidentally or deliberately compromised

Data protection reform -

The ***General Data Protection Regulation (GDPR)*** became law on 24 May 2016 and will be implemented on 25 May 2018 when it replaces the Data Protection Act 1998.

The GDPR will require organisations to put stronger controls and processes in place to protect the security and confidentiality of personal data.

Key changes

- Expanded scope
- New information right
- Breach notification
- Stronger enforcement
- Data Protection Officers
- Higher standards for consent
- Data protection by design and Data Protection Impact assessments
- Accountability

Information Security

Everyone has individual responsibility for ensuring that personal data is kept secure and confidential. Failure to protect personal information will lead to a breach of the seventh data protection principle.

Physical Security

- Shut/lock doors & cabinets
- Wear ID badges
- Query the status of strangers
- Report anything suspicious
- Do not divulge security systems
- Don't leave information unattended in unsecure locations
- Don't discuss personal information where you can be overheard
- Don't copy or remove (take offsite) personal or business confidential information without authorisation

- Use confidential waste disposal for paper records containing personal information
- Special care must be taken when disposing of data devices. Equipment must be returned to the IT Department for recycling or secure destruction. Equipment such as desktop computers; laptops; tablets; mobile phones; digital records; cameras; USB devices, CDs/DVDs

Passwords

Did you know that weak password security is still the main cause of data loss?

To protect the systems you use you should choose a strong password for **each** system you use that meets the Trust's password requirements. Passwords shouldn't be written down or be shared with anyone else. When changing your password make sure it is significantly different from the previous password. Always follow the Trust's password requirement when setting passwords even for use on systems that don't currently have length and complexity constraints.

LHCH password requirements:

- *Must be a minimum of 8 characters and contain the following:*
  - *An uppercase letter*
  - *A lowercase letter*
  - *A number*
  - *A special character such as @#$%^&£*

Passwords should not contain easily guessed information such your birth date, phone number, spouse's name, pet's name, child's name, login name, etc. Or just contain words found in the dictionary

Computers

- Only access confidential data when you need to as part of your job. It is illegal to access for personal reasons
- Position your computer screen to avoid unauthorised viewing
- Lock your computer before moving away from your desk - press the 'Windows + L to quickly secure your PC
- Never store personal or confidential information on unencrypted USB data sticks, laptops or other portable media.
- Do not use unauthorised USB drives - the Trust can provide encrypted sticks if required
- Do not plug in any non-approved devices to charge via USB cable
- Scan USB data sticks before use - Simply open 'My Computer' and right click on the device or volume and select 'Scan with anti-virus' from the drop down menu

Mobile devices

- Read, understand and comply with Trust policy & procedures (ISMS security standards)
- Set passcodes on corporate mobile devices and activate the lock function
- Store your digital assets securely when not in use
- Don't use your own personal devices for business purposes or your business devices for personal use unless authorised
- Update antivirus software, if prompted there's an update available contact the IT department
- Don't connect devices to unknown or untrusted networks e.g. public WiFi hotspots
- Don't connect unauthorised equipment of any kind to your business device; computer or network
- Don't store confidential information or data on mobile devices
- Don't copy or remove (take offsite) personal or business confidential information by email or USB data stick without authorisation

- Don’t install unauthorised software or download software or data from the internet
- Don’t disable antivirus protection software
- Any lost or stolen devices must be reported immediately through the Trust’s incident reporting system. Incidents involving patient/person identifiable or business confidential information stored on unsecured devices should also be reported to the Information Governance Manager.

Cyber security

Cyber-attacks cost organisations thousands of pounds and cause lengthy disruption to services. All businesses are at risk of a cyber-attack including the NHS. A serious cyber-attack forced Northern Lincolnshire and Goole NHS Foundation Trust to shut down most of its network and cancel operations & appointments in October 2016. Systems remained down for four days following the attack.

Many NHS Trusts were caught up in and affected by the major international cyber-attack (Wannacry ransomware attack) that caused widespread disruption in May 2017.

The Trust follows the Government backed Cyber Essentials Scheme and has implemented a number of technical solutions to help protect against attacks. This includes use of anti-virus software to prevent, detect and remove malicious software; firewalls to prevent unauthorised access to our network, secure configuration of our network and systems supported by robust patch management (carrying out regular software upgrades) and restricting access to applications to those who need it.

Social engineering

This is the psychological manipulation of people into performing actions or divulging confidential information. This could involve confidence tricks or the interception or theft of devices or documents used to gain further access to protected systems.

on the phone

- a social engineer might call and pretend to be a fellow employee or a trusted outside authority

in the office

- "can you hold the door for me? I don't have my key/access card on me" a common tactic used by social engineers

online

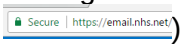
- social engineers routinely use social networking sites, they steal passwords, hack accounts and pose as 'friends' for financial gain.

Email phishing and malware

This is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Phishing emails are another example of social engineering and may contain links to websites that are infected with malicious software (malware).

Malware can be on your computer and evade detection allowing someone to be active on your system with you noticing. Malware can make your computer run slowly or perform in unusual ways.

Cyber security what to do

- Always be vigilant
- Look out for spoof emails (email addresses can be made to appear as if they've come from someone you know) – where a message is unexpected or unusual check with the person using another method
    - Don't open attachments or click on links within any unsolicited emails you receive
    - Don't respond to emails that ask for personal or financial details
    - Delete suspect messages immediately
    - Report the incident and notify the IT Department contact our IT Security Officer by email: ITSecurity@lhch.nhs.uk or phone: ext. 1525
- Make sure the website address you are visiting is the correct address and that it is secure (https:// or the padlock is displayed e.g. 

)
- Be very careful if a web browser states that you're about to enter an untrusted site
- Look out for a red padlock or a warning message stating 'your connection is not private'
- Use strong passwords and do not reuse previous passwords
- Don't divulge your password to anyone … this includes callers claiming to be from our IT department
- Challenge strangers, if it's safe to do so, and ask for proof of identification
- Do not enable Macros unless you trust the source document … Macros can be programmed to install malware

Disclosing information

- Disclose information on a 'strict need to know' basis and use only the minimum personal data required
- Follow the requirements of established Information Sharing Agreements and remember the Data Protection & Caldicott principles
- Follow safe haven procedures for the secure receipt and despatch of confidential information
- Choose the most appropriate and most secure transfer method when disclosing personal information, for example encrypted email, safe haven fax, track & trace mail etc.

Data protection breaches and incidents

Incidents typically fall into two categories:

- A breach of one of the principles of the Data Protection Act and/or confidentiality law
- Technology-related incidents

The table below gives some examples:

Breaches	Cyber incidents
Identifiable data lost in transit	Phishing email
Lost or stolen hardware	Denial of service attack (an attempt to make a machine or network resource unavailable to its intended users)
Lost or stolen paperwork	Social media disclosure (disclosure of confidential or sensitive information by employees on their personal social media site e.g. Facebook; Twitter)
Data disclosed in error	Website defacement (an attack on a website that changes the content)
Data uploaded to website in error	Malicious damage to systems (when a person intentionally sets out to corrupt or delete electronic files, information or software programs)
Non-secure disposal – hardware	Cyber bullying
Non-secure disposal – paperwork	
Technical security failing	
Corruption or inability to recover data	
Unauthorised access or disclosure	

Data shows that the most reported breaches in health and care are:

- Faxes that are sent to the wrong number
- Lost or stolen paperwork
- Failure to adhere to principle seven of the Data Protection Act

Incident reporting

All incidents, possible breaches or near misses involving personal information must be formally reported using the Trust's online Incident Reporting tool - *Intranet homepage > Essential Links > Incident Reporting*.

Reports should be entered under the *Information Governance* category, with the relevant sub-category selected from the drop-down list. The following information should be included and Wyn Taylor, IG Manager should be assigned as the *Incident Handler*:

- Date, time and location of the incident
- Description of what happened:
    - Theft, accidental loss, inappropriate disclosure, procedural failure; lost in transit etc.
    - The number of records / individuals involved
    - If electronic, whether the data had been encrypted or not
    - The type and sensitivity of record / data involved e.g. name, address, medical condition
- Immediate action taken
- Contact details of incident reporter

The Information Commissioner's Office (ICO)

The UK's independent authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

Part of the ICO's role is to take action to ensure organisations comply with legislation and meet their information rights obligations. They have various enforcement powers including the ability to impose financial penalties of up to £500,000 for serious data breaches and to initiate criminal prosecutions.

Unlawfully obtaining or accessing personal data is a criminal offence under Section 55 of the ***Data Protection Act 1998*** and is punishable by way of an unlimited financial penalty. Action in such instances can be taken against the individual who accesses the data unlawfully.

During the last 12 months enforcement action has been taken by the ICO on 13 occasions within the health sector, including three prosecutions and three monetary penalties:

▪ ***April 2017*** – Prosecution of a former clerical officer for accessing medical records without consent/authorisation when employed by an NHS hospital trust ▪ ***March 2017*** – Prosecution of a former nurse for accessing sensitive medical records when employed by a Health Board ▪ ***October 2016*** – Prosecution of a former administrative employee for accessing medical records without consent/authorisation when employed by an NHS hospital trust	▪ ***February 2017*** – Monetary penalty of £200,000 issued to a private health company for failing to keep fertility patients' personal information secure (unsecured server resulting in data being available online) ▪ ***August 2016*** – Monetary penalty of £15,000 issued to a nursing home for failing to keep sensitive personal data secure (theft of an unencrypted laptop containing confidential information) ▪ ***August 2016*** – Monetary penalty of £40,000 issued to a GP practice following a unauthorised disclosure of personal data without consent (sensitive information disclosed to a third party)

Record Keeping and data quality

- Accurate
- Relevant
- Complete
- Accessible
- Timely
- Free from duplication
- Defined
- Appropriately stored
- Appropriately sought

It is important that records are full, accurate, dated and timed. We need to collect all relevant information ensuring that all mandatory items are captured. Records should be written at the time of an event occurred or as soon after as possible and should be stored securely and protected from inappropriate access.

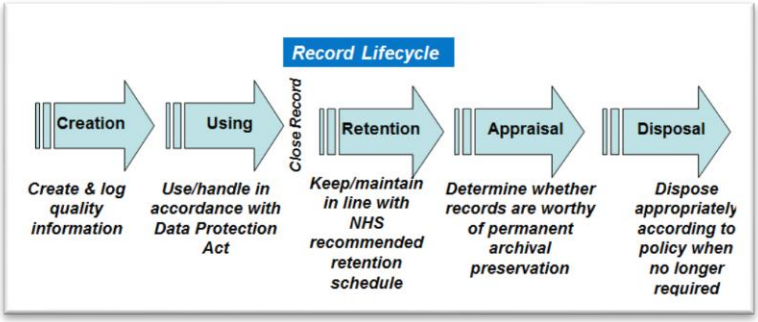
Checks should be made to avoid creating duplicate records and individuals should be given the opportunity to check and confirm the details held about them.

Records need to be readily available – movement of paper case notes must be tracked; supporting paper documents should be scanned or uploaded into the patient's EPR record.

Record Management

All NHS 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 request requirements under Data Protection and Freedom of Information (FOI) and legislation.



Requests for Information

Requests for information are coordinated centrally for the Trust and requests must be date stamped and forwarded on the day of receipt to Information Governance.

Corporate information

The ***Freedom of Information Act 2000 (FOIA)*** provides the public with a general right of access to non-personal information held by public authorities.

Requests must be made in writing (letter, email, fax) and held information means information that is recorded in the organisation's corporate records for example in a document; in a spread-sheet or database, in an email etc. There is no requirement to create new information to respond to requests but if held, the relevant information must be released within 20-working days unless an exemption applies.

FOI requests should be forwarded immediately to the IG Team at FOIRequests@lhch.nhs.uk

Personal information including health records

The ***Data Protection Act 1998 (DPA)*** grants rights for living individuals to access their own records, this is known as Subject Access. The right can also be exercised by an authorised representative on the individual's behalf.

The ***Access to Health Records Act 1990 (AHRA)*** grants rights of access to deceased patient health records by specified persons primarily the legally appointed personal representative e.g. Executor of the estate.

The ***Medical Reports Act 1988*** grants a right for individuals to have access to reports relating to them provided by medical practitioners for employment or insurance purposes.

Requests for personal information must be made in writing and be accompanied with formal proof of identification and where applicable, proof of right of access and patient consent. The Trust does not routinely charge for processing requests for access to health records however a charge could be applied where there is potential disproportionate effort to comply with a request.

The Trust's standard application form can be used and is available on the intranet. Requests must be processed within 40-calendar days of receipt.

Requests for personal information should be forwarded immediately to the IG Team at infogov@lhch.nhs.uk.

Your IG responsibilities

- Keep all personal and sensitive information secure
- Be vigilant to cyber security treats (phising emails etc.) and always follow security procedures (safe haven, encryption etc.)
- Record information accurately and ensure it is accessible when needed
- Use and share information appropriately and lawfully
- Be aware of the Data Protection and Caldicott principles
- Respect the rights of individuals and comply with access to information requirements
- Report breaches of security, suspected or actual incidents or concerns

- Keep up to date with Trust IG & ISMS policies

Where to go for more guidance

Information Governance intranet

Home > Departments > Corporate Services > Information Governance

- Confidentiality and Data Protection
- Freedom of Information
- Information Risk Management and Information Security
- Information Governance Policies and Procedures
- Information Governance Templates
- Record Management
- Training and Awareness

IG policies

Intranet home > Policies and Procedures > Non-clinical

- Code of Conduct for Handling Personal-identifiable information
- Data Quality policy
- Health records and case note management policy
- Information Governance policy
- Information Disclosure policy
- Information Risk policy

ISMS policy and security standards

1. IG and safe haven
2. Security control of assets
3. Access control to secure areas
4. Equipment Security
5. Computer and network operations
6. System planning, procurement and acceptance
7. Protection from malicious software
8. Housekeeping
9. Data and software exchange
10. Monitoring system access and use
11. User access control – password policy
12. Computer access control
13. Application access control
14. Data Validation
15. Security of application systems
16. Security incident management
17. Forensic readiness
18. Risk assessment
19. Business continuity planning

IG Team

- Liam McCormack, IG Facilitator - Ext. 1845 Liam.McCormack@lhch.nhs.uk
- Carol Taylor, IG Officer - Ext. 1240 Carol.Taylor@lhch.nhs.uk
- Wyn Taylor, Information Governance & Health Records Manager, Ext. 1368 Wyn.Taylor@lhch.nhs.uk

IT Security

- Gemma Owens, IT Security Officer - Ext. 1525 Gemma.Owens@lhch.nhs.uk

Caldicott Guardian

- Dr Raph Perry, Deputy Chief Executive and Medical Director - Ext. 1429 Raphael.Perry@lhch.nhs.uk

Senior Information Risk Owner

- Dr Mark Jackson, Director of Research & Informatics - Ext. 1332, Mark.Jackson@lhch.nhs.uk

ACTIVITY: Information Governance

Do not forget to complete the on-line assessment via the Intranet (see page 1 of the e-leaning quick start guide).

Please note:

- If you achieve 83% or more you have been successful
- If you do not achieve 83% you will not be deemed as compliant with your essential mandatory training and will need to repeat the test
- You must ensure you are compliant annually for IG training