HEM ULTRASOUND

INFORMATION GOVERNANCE

AGENDA 2019

(Version 2)

AUTHOR	Date	AUTHORISER	Date
Emma Streater – Service Director	04/03/2019	Heather Moores – Managing Director	04/03/2019
Date of next review: March 2020			

HEM ULTRASOUND INFORMATION GOVERNANCE AGENDA

INDEX

OVERVIEW OF INFORMATION GOVERNANCE

This policy should be treated as the overarching agenda for all risk assessments and protocols concerned with or related to information governance to enable assurance of the company's compliance with statutory, legal and insurance requirements to support standardisation of practice for all staff who work for on behalf of the company.
In order to ensure that there is a robust information governance framework for the company that enables assurance that patient and staff confidentiality is maintained the policy must follow the standards and legal requirements outlined in:

- The Data protection act 1998
- Caldicott report
- Common law duty of confidentiality
- General Data Protection regulations (GDPR)
- NHS England Confidentiality policy, 2014 (version 2.0, document number POL_1010)
- Freedom of information act 2000

As the company will be dealing with patient data, all staff working for or on behalf of the company are bound by a legal duty of confidence as outlined in the data protection act 1998 and the NHS confidentiality policy, 2014. However, the overarching responsibility of ensuring full staff and company compliance with information governance (IG) policies and protocols lies with the Directors of the company. It is the company's responsibility as an entity to ensure that it safeguards and preserves confidential information security at all times.

INFORMATION GOVERNANCE ROLES & ACCESS

RED – FULL ACCESS TO SERVICE INFORMATION BARRING NO EXCEPTIONS
GREEN – FULL ACCESS TO PATIENT, STAFF, BUSINESS SERVICE PROVIDER AND COMPANY POLICIES AND PROCEDURES WITH EXCLUSIONS.
PURPLE – ACCESS TO ONLY CLINIC LISTS AND PATIENT INFORMATION ON THE DAY DATA.
BLUE – THIRD PARTY PROVIDER ACCESS TO VIEWED INFORMATION THROUGH THE COURSE OF THEIR WORK, DATA CONFIDENTIALITY AGREEMENTS IN PLACE.

SENIOR INFORMATION RISK OWNER

Heather Moores – MANAGING DIRECTOR/ Lead Clinician – Sonographer practitioner

ACCESS LEVEL – ACCESS TO ALL SERVICE INFORMATION
As the managing director, they have access to all information regarding the service as is necessary to perform their role.

The SIRO will take overall ownership of the Clinics Information Risk Policies. The SIRO is expected to understand how the strategic business goals of the clinic and how other NHS Organisations' business goals may be impacted by information risks, and how those risks may be managed.
The SIRO will implement and lead the Clinic's Information Governance (IG) risk assessment and management processes.

The SIRO shall receive training as necessary to ensure they remain effective in their role as Senior Information Risk Officer. Oversee the development of an Information Risk Policy. Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the IG lead, Caldicott guardian and all clinic staff.
To:

- Review and agree actions in respect of identified information risks.
- Ensure that the clinic's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Provide a focal point for the escalation, resolution and/or discussion of information risk issues.
- Ensure that an effective infrastructure is in place to support the role by developing a simple Information assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities
- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG requirements.
- To ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.
- Provide leadership, sharing of relevant experience, provision of training and creation of information risk reporting structures.
- Advise on the level of Information Risk Management performance within the Clinic including potential cost reductions and process improvements arising
- The SIRO holds overall responsibility for ensuring privacy impact assessments are carried out regarding all aspects of personal and sensitive information held by the clinic.
- The SIRO is responsible for ensuring robust Data processing agreements are in place with organisations processing personal and sensitive information outside of the service. Ensuring these agreements are completed at the same time as privacy impact assessments and in line with the requirements of the Data Protection Act 1998 and in line with the General Data Protection Regulations.
- To develop and implement procedures to ensure that all routine uses of person-identifiable patient information are identified, agreed as being justified and documented.

- To establish Information Sharing Protocols to govern the use and sharing of person-identifiable patient information between organisations both within and outside the NHS.
- To ensure standard procedures and protocols are in place to govern access to person-identifiable patient information.
- User access controls – responsible for ensuring staff have access to information that is appropriate only for their role, specifically access to e-clinic is restricted to enable them only to complete their duties.
- To ensure passwords are changed regularly for e-clinic and for computers and that staff are not disclosing their passwords.
- To ensure no e-mail accounts are left with saved passwords and are single entry only.

CLINICAL GOVERNANCE

- The SIRO responsible for the clinical audit structure and publication. In addition, their role is to enable a clear audit feedback dialogue with Clinicians and our information sharing partners. As well as ensuring any findings of clinical errors are flagged and shared with clinicians and referrers involved in the patients care, and are fully investigated if a RIDDOR Event.
- Clinic Activity performance reviews assess levels of activity within the clinic by patients from individual CCG's. this is carried out every month and fed back to the CCG's for their records.
- As lead clinician it is their responsibility to ensure patient data accuracy and quality when undertaking their role.
- Continually monitor and bench mark clinic IG standards against IG tool kit requirements and make improvements when required to maintain high levels of compliance.

ALL INFORMATION ASSETS TO OVER SEE ASSIGNED TO THE SIRO:

- E-clinic patient management database
- Clinical Audits
- Anonymised billing records for CCG's and Hospital trusts
- Company Financial Records
- Personnel files and training records
- Results of patient satisfaction questionnaires
- Business contracts services and provisions database.
- Company policies procedures and meeting notes

DATA PROTECTION OFFICER - Responsibilities

Emma Streater – Service Director:

ACCESS LEVEL – ACCESS TO ALL SERVICE INFORMATION
The DATA PROTECTION OFFICER has access to all information necessary to undertake their role, and for that reason extends to all information assets, private and confidential information.

The Data protection Officer is expected to understand how the strategic business goals of the clinic and how other NHS Organisations' business goals may be impacted by information risks and advise how those risks may be managed. The Data protection officer will implement and carry out a schedule for Data Privacy Impact Assessments. The Data Protection Officer shall receive training as necessary to ensure they remain effective in their role.

To:

- Review and advise actions in respect of identified information risks.

- Ensure that the clinic's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Assisting the SIRO to help develop an effective infrastructure to support the role by developing a simple Information assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities
- Ensure that identified information threats and vulnerabilities are followed up to advise risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG requirements.
- To monitor and advise on mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.
- Provide leadership, sharing of relevant experience, provision of training and creation of information risk reporting structures.
- Advise on the level of Information Risk Management performance within the Clinic including potential cost reductions and process improvements arising
- Working with the SIRO to ensure privacy impact assessments are carried out regarding all aspects of personal and sensitive information held by the clinic.
- Working with the SIRO to ensure data processing agreements are in place with organisations processing personal and sensitive information outside of the service. Ensuring these agreements are completed at the same time as privacy impact assessments and in line with the requirements of the Data Protection Act 1998 and in line with the General Data Protection Regulations.
- Be responsible for reviewing current policies and procedures when they become due for review, amend where required and write new policies and procedures when necessary.
- Keeping up to date on relevant legislation changes and updates which may affect the information governance provisions within the service. Looking specifically at the GDPR and the Data protection act and local and national guidance from the Information commissioner's office.
- This person is also responsible for overseeing all company financial dealings and data, primarily cash flow, payroll and invoicing. Ensuring that the clinic retains funds for continual progression and development and that financial assets are reinvested in the company to ensure its longevity and quality of service.
- Develop and maintain IG training and staff induction and updates for all staff, ensure all staff are made aware of any changes to the law or policies that affect IG within the clinic.
- To ensure passwords are changed regularly for e-clinic and for computers and that staff are not disclosing their passwords.
- To ensure no e-mail accounts are left with saved passwords and are single entry only.
- To check anti-virus software is up to date and run a full scan once a month to check for any issues on all the 1st floor office computers.

ALL INFORMATION ASSETS TO ADVISE ON:

- E-clinic patient management database
- Clinical Audits
- Anonymised billing records for CCG's and Hospital trusts
- Company Financial Records
- Personnel files and training records
- Results of patient satisfaction questionnaires
- Business contracts services and provisions database.

- Company policies procedures and meeting notes

CALDICOTT GUARDIAN

Tina Potts – Operations Manager

ACCESS LEVEL – ACCESS TO ALL SERVICE INFORMATION
As Operations manager, they have access to all avenues of the business so together with the Managing Director and Service Director. Make up one third of the company's senior managers.

In addition to the principles developed in the Caldicott Report, the Guardian must also take account of the codes of conduct provided by professional bodies, and guidance on the Protection and Use of Patient Information and on IM&T security disseminated by the Department of Health.
To provide advice and support to staff working within the Clinic on all aspects of Caldicott, sharing and disclosure of person-identifiable patient information and related legislation.

Main roles are:

- Be the conscience of the clinic on all matters to do with patient data protection.
- Collaboration on Information Governance procedures, guidelines and protocols, with the SIRO.
- To develop and implement criteria and a process for dealing with ad hoc requests for person-identifiable patient information for non-clinical purposes.
- To ensure standard procedures and protocols are in an understandable format and available to staff
- Raise awareness through training and education to ensure that the standards of good practice and Caldicott principles are understood and adhered to.
- To bring to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed.
- To raise concerns about any inappropriate uses made of patient information with the SIRO and Managing Director where necessary.
- On an annual basis, to participate in the Information Governance Toolkit Assessment.
- Advise the SIRO and the IG lead on all aspects of processing person-identifiable patient information.

HR Information quality assurance – to be responsible for ensuring HR Records are up to date and relevant data is held for each staff member including: CV, DBS check, Copies of identification, Training certificates, Sign sheets for policies read and understood.

- Liaise with CEO/SIRO on a monthly basis or when required to ensure clarity and good communication is upheld.
- Ensure that there is clarity for the public, service users and clients about how the clinic ensures compliance with the Data protection act 1998 and the Freedom of information act 2000
- Assist the SIRO in any complaints related to IG such as breaches of confidentiality. Assist in any investigation and reporting of such incidents. Play a major role in implementing remedial action if required.

INFORMATION ASSETS ASSIGNED TO THE CALDICOTT (IAO) ARE AS FOLLOWS:

- Personnel files and training records

- Anonymised billing records for CCG's and Hospital trusts

ADDITIONAL ROLES:

The SIRO, Data Protection Officer and Caldicott Guardian hold seniority in ownership of information risk management. However, the company allocates responsibility to every member of staff within the service, to ensure that each member of the team has a role within the framework and therefore a vital responsibility to our IG agenda.
The following information governance responsibilities are allocated and undertaken by all staff on a regular basis, and some assigned ad hoc to meet the needs of the service:

- Key responsibility for all staff to ensure patient data accuracy and quality when undertaking their role.
- Computer spot checks of scan room and reception. This includes ensuring recycle bin and the downloads folder is empty and all confidential data has been uploaded to e-clinic and then deleted from the computers.
- To check computers are not left unattended with patient information on the screen, within easy sight of visitors.
- Computers in the scan room and reception should not contain any data that is confidential. It is every staff members' responsibility is to spot check both computers to ensure that no data is saved to the computer.
- If data is found that shouldn't be there is the responsibility of the staff member to take note of what information has been found, where it was found and report it immediately to the Clinic Operations Manager for investigation.
- Patient information quality checklists. This responsibility involves, every day, using a specially designed check sheet to assess for information quality on e-clinic. The check sheet asks for the responsible person to check that the most important information has been attached to the patient profile. This includes: referral form, consent form, images, scan report, fax/e-mail confirmation of the returned report and if the patient has DNA'd – information regarding additional correspondence or referral back to GP.
- If any errors data accuracy and quality are found to inform the Operations Manager/IG lead.
- Ensuring the clinic reception contains no accessible patient or staff information, by routinely carrying out visual spot checks of drawer's, desks and office area.
- To be vigilant in ensuring no confidential information is verbally discussed in the waiting area and reception by staff in front of patients, if breaches occur to report directly to the clinic Operations manager to ensure culpable parties are informed of the breach and a confidentiality breach investigation implemented.
- Checking all cleaning checklists are updated on a daily basis, if they are not this needs to be flagged to operations manager to ensure any persons not completing their responsibilities are informed and it is rectified.
- To maintain an ongoing log of infection control check sheets for the whole clinic, dated for ease of access.
- To include up to date policies on infection control in the log book found in the clinic scan room.
- To ensure they abide by their information governance training and ensure they conduct their roles under the clear supervision of the senior clinic management team.

Jordon Creasey – Trainee IG Officer

ACCESS LEVEL - LIMITED TO STAFF, SERVICE USER INFORMATION AND PRACTICE MANAGEMENT PROVISIONS.
As IG officer their role requires them to have access to staff files, service user information – but only when legitimately required for administrative tasks. In addition access to the clinics contacts list for service providers is essential.
This role does not require access: to financial information regarding the company.

The role of the Information Officer is to coordinate, promote and monitor the standards of information handling within the clinic, ensuring that employees are fully informed of their own responsibilities for maintaining the standards within the clinic. Further ensure secure information handling is monitored for all third-party contractors.

- The IG Officer must ensure that IG issues are discussed at all clinic Governance meetings.
- Assist the SIRO, in annual assessments of the clinic's performance against the IG tool kit requirements, support all staff in ensuring the highest standards are continually met.
- Ensure Clinical Audits requests are sent to external Auditors – Medica Reporting Group LTD with the correct level of anonymisation.

INFORMATION ASSETS ASSIGNED TO THIS IAO ARE AS FOLLOWS:
Clinical Audit lists and Communication

Deputy Clinic Manager – Karen Murray

ACCESS LEVEL - LIMITED TO STAFF, SERVICE USER INFORMATION AND PRACTICE MANAGEMENT PROVISIONS.
As Deputy Clinic manager their role requires them to have access to staff files, service user information – but only when legitimately required for administrative tasks. In addition, access to the clinics contacts list for service providers is essential.
This role does not require access: to financial information regarding the company.

SONOGRAPHERS/CLINICIANS

ACCESS LEVEL – LIMITED TO DAILY CLINIC LIST INFORMATION.
This member of staff is only allowed access to information necessary to perform their role on a daily basis. Such as: patients booked for scans, their clinical indication. They are required to have access to all policy documentation regarding the service, to ultimately support their role.

This role does not require access to:

Patient Image archives, Clinical Audits, Anonymised billing records for CCG's and Hospital trusts, Company Financial Records, Personnel files and training records, Results of patient satisfaction questionnaires, Business contracts services and provisions database.

Apprentices & Clinic Assistants

ACCESS LEVEL – LIMITED TO DAILY CLINIC LIST INFORMATION.
This member of staff is only allowed access to information necessary to perform their role on a daily basis. Such as: patients booked for scans, their medical history preparation. They are required to have access to all policy documentation regarding the service, to ultimately support their role.

This role does not require access to:

- Patient Image archives
- Clinical Audits
- Anonymised billing records for CCG's and Hospital trusts
- Company Financial Records
- Personnel files and training records
- Business contracts services and provisions database.

SUBCONTRACTORS

E-Clinic (E-Dataware LTD)

E-clinic is the clinics patient management system. On which all patient data is stored. The patient data is accessed remotely via a two password, secure remote connection via the internet. Upwards of 26,000 patient's information is stored on e-clinic.
E-clinic (E-Dataware LTD) and HEM ultrasound have an annually renewed Data processing agreement which contains details of both parties' commitment to the requirements of the Data Protection Act 1998 and the General Data Protection Regulations. The agreement outlines activity undertaken on behalf of the company and the type of data transferred and processed.

Data Privacy Impact assessments are undertaken annually to ensure the control measures are still supporting the purpose and security of the agreement.
Data Processing Agreement and Data Privacy impact assessments are referenced in the Appendices

Medica Reporting Group Limited

Medica Reporting group Limited are an external provider of clinical auditing services. We send a monthly audit of 5% of total ultrasound examinations, these examinations are audited by consultant radiologists.
Medica is connected directly to our ultrasound scanners via a secure firewall protected network. We send patient images selected for audit direct to Medica via Dicom transfer. The anonymised patient lists are sent to medica via NHS e-mail for the auditing radiologists to reference. The auditing radiologists then have access to e-clinic to compare the report with the images.
Medica Reporting Group LTD and HEM ultrasound have an annually renewed Data processing agreement which contains details of both parties' commitment to the requirements of the Data Protection Act 1998 and the General Data Protection Regulations. The agreement outlines activity undertaken on behalf of the company and the type of data transferred and processed.

Data Privacy Impact assessments are undertaken annually to ensure the control measures are still supporting the purpose and security of the agreement.
Data Processing Agreement and Data Privacy impact assessments are referenced in the Appendices

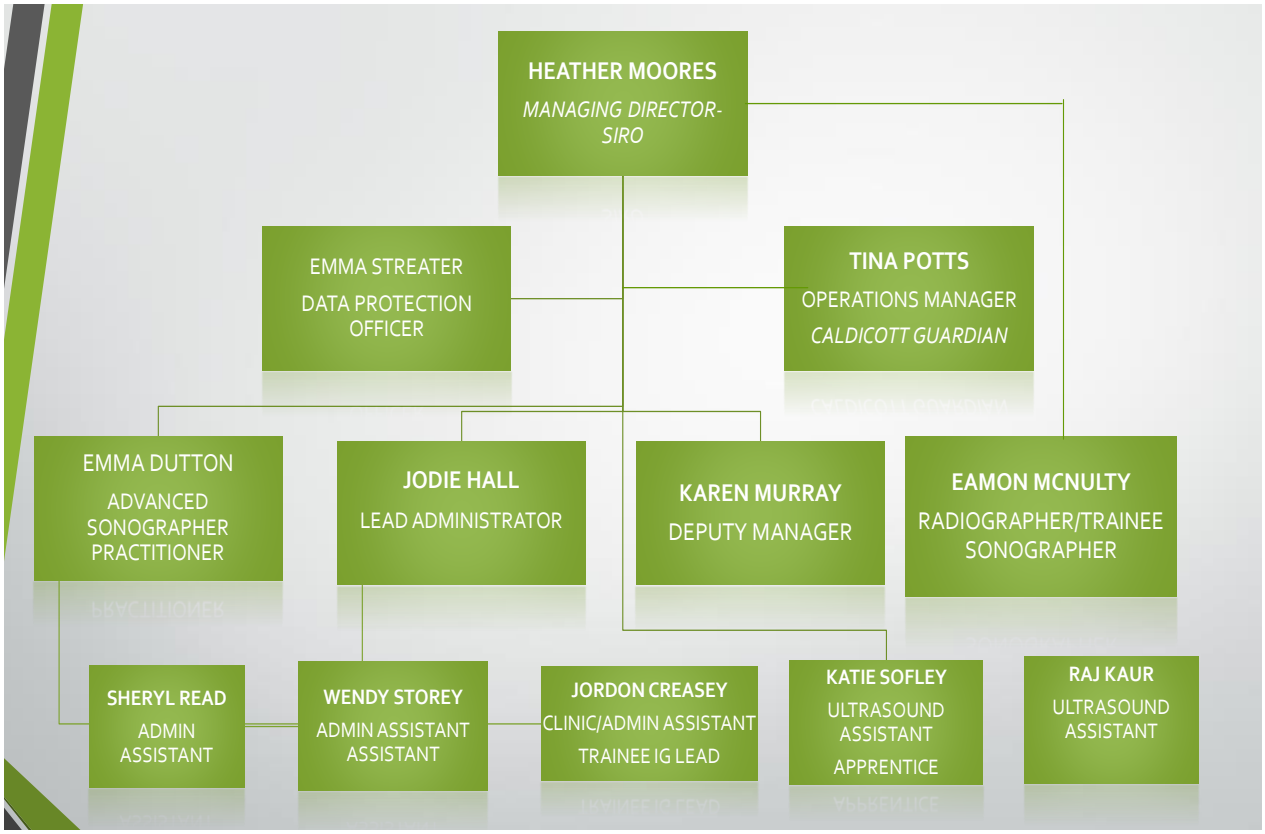
Jeff Earle
Information Governance Responsibilities on behalf of HEM Ultrasound a third party provider:

- Provide IT support when issues arise such as virus detection.
- Provide support implementing new IT solutions
- Provide support issuing new user profiles and monitoring user activity for audit purposes

Overall protection of staff and service user information as well as information assets are divided between staff members however it is the responsibility of every member of staff to ensure they are maintaining the companies IG agenda and flag issues immediately with the SIRO and Operations Manager.
Jeff Earle and HEM ultrasound have an annually renewed Data processing agreement which contains details of both parties' commitment to the requirements of the Data Protection Act 1998 and the General Data Protection Regulations. The agreement outlines activity undertaken on behalf of the company and the type of data transferred and processed.

Data Privacy Impact assessments are undertaken annually to ensure the control measures are still supporting the purpose and security of the agreement.

IG MANAGEMENT FRAMEWORK STRUCTURE CHART:



WHAT IS CONFIDENTIALITY AND DATA PROTECTION? & WHAT DIFFERENCE DOES THE GDPR MAKE?

The aim of this segment is to outline what constitutes 'data' and what specific 'data' need's robust procedures in place to ensure that it is protected. We will highlight the processes in place that protect IT data assets from malicious or accidental breach. In addition we will look at protocols in place for hardcopies of confidential data (paper files).

The GDPR (General Data Protection Regulation) came into force on the 25th May 2018. The GDPR are European regulations created by the EU and is applicable to member states. The Government has confirmed the regulations will still be applicable to UK data controllers despite leaving the EU. The Data protection Act of 1998 is still relevant however the GDPR expands on certain aspects and enables regulatory bodies to enforce more legal responsibilities to data controllers (persons responsible for confidential data) and Data processors (persons responsible for utilising data in their activities). The GDPR like the Data Protection act 1998, sets out clear rules for the processing and use of protected data.

For HEM Clinical Ultrasound service limited, protected data will be classed in the following categories**:**

- **Personal data** (Person Identifiable data). Which would be in brief is any data used for identification purposes
  - Name
  - Date of Birth
  - Address
  - NHS number etc.…

- **Sensitive personal data:** this is any data that can be reasonable used to discriminatory and defamatory effect by a person(s). Which would consist of:

  - Ethnic or racial origin
  - Political beliefs
  - Religious beliefs (or similar subjects)
  - If they are a member of trade union
  - Details of their physical or mental health
  - Sexual orientation or activity
  - Past convictions or legal proceedings

It is our responsibility as a company handling personal data and sensitive personal data to ensure that it's protected appropriately.

We must establish the legal terminology used to compartmentalise how data is itemised and used. To clarify: ***Data subjects*** *(*patients and staff) have all their data processed by the ***Data Controller*** (HEM Clinical Ultrasound service limited) and those senior managers acting in the *Controller* capacity. Data is then passed from the controller to the ***Data Processors*** (Admin team, Clinic manager, Receptionist, Ultrasound assistant and Sonographer or Radiologist) who need to utilise the data in order to undertake their employed purpose. If a member of staff has been asked by a manager or Data controller to utilise personal/sensitive data for a purpose not specified by their set role or job description they would become a ***Third party***.

When handling personal/sensitive data we have to abide by the Data Protection Act 1998 and the new rules put in place by the General Data Protection Regulations. We will look specifically at the following principles when handling personal and/or sensitive information and how the GDPR affects these principles

(Principles and explanations taken from the ICO guidance '*The Guide to Data Protection' and The Data Protection Act 1998,* identified in blue and 'Preparing for the GDPR 12 Step process' in Green).

DATA PROTECTION PRINCIPLES

PRINCIPLE 1:
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- *The individual whom the personal data is about has consented to the processing.*

The GDPR - The Information commissioner's office advises:
Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

- *The processing is necessary in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.*
- *The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).*
- *The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.*
- *The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.*
- *The processing is in accordance with the "legitimate interests" condition.*

In addition principle 1 sets out the following points, which we must:

- *have legitimate grounds for collecting and using the personal data*
- *not use the data in ways that have unjustified adverse effects on the individuals concerned;*
- *be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;*
- *handle people's personal data only in ways they would reasonably expect; and*
- *make sure you do not do anything unlawful with the data.*

Patients are consenting to the use of their personal information by going to the doctor as the doctor would reasonably arrange a scan as part of on-going care and would be expected to be part of the Dr – Patient agreement. So codes of confidentiality are expected and carried across

from GP's surgeries with regard to patient referral, the same applies to referrals from midwives and nurse practitioners. Patients who self-refer give their information and consent to use it as part of employing our service for their care.

The GDPR - The Information commissioner's office advises:
'*You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it. Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing. You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements*'

As part of maintaining transparency on how we will be handling data we have put in place a privacy notice or 'How we use your information' disclaimer so patients have no surprises as to how their data is handled and for what lawful purpose.

PRINCIPLE 2:
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- *be clear from the outset about why you are collecting personal data and what you intend to do with it;*
- *comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;*
- *comply with what the Act says about notifying the Information Commissioner; and*
- *Ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.*

We will always be clear as to why we need to use patient data, as this is reasonably implicit as we would have received a referral from a practitioner a practitioner for healthcare purposes. However, if we at a future date wish to utilise the patient data for healthcare research purposes for an external company with a non-marketing agenda, we would always ask for patient's written permission and be explicit as to how their data will be used.

The GDPR - The Information commissioner's office advises:
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

PRINCIPLE 3.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

This is the third data protection principle. In practice, it means you should ensure that:

- *you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and*
- *you do not hold more information than you need for that purpose.*

We will only have the capacity to store data that is specific for the purposes of the clinic. Patient identifiable data would be purely for appointing and patient sensitive data would be referrals, reports and images only. In special circumstances for example: an accident, or safeguarding incident, we would also hold details of the incidents on the patient database for auditing purposes.

The GDPR - The Information commissioner's office advises:

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas. The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

PRINCIPLE 4:

Personal data shall be accurate and, where necessary, kept up to date.

'To comply with these provisions you should:

- *Take reasonable steps to ensure the accuracy of any personal data you obtain*
- *ensure that the source of any personal data is clear carefully consider any challenges to the accuracy of information*
- *Consider whether it is necessary to update the information'*

When considering diagnoses and clinical opinion being 'accurate' we should look to the following excerpt from 'The Guide to data protection' ICO:

> *'An area of particular sensitivity is medical opinion, where doctors routinely record their opinions about possible diagnoses. It is often impossible to conclude with certainty, perhaps until time has passed or tests have been done, whether a patient is suffering from a particular condition. An initial diagnosis (or informed opinion) may prove to be incorrect after more extensive examination or further tests. Individuals sometimes want the initial diagnosis to be deleted on the grounds that it was, or proved to be, inaccurate. However, if the patient's records accurately reflect the doctor's diagnosis at the time, the records are not inaccurate, because they accurately reflect a particular doctor's opinion at a particular time. Moreover, the record of the doctor's initial diagnosis may help those treating the patient later'.*

PRINCIPLE 5:
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

This is the fifth data protection principle. In practice, it means that you will need to:

- *Review the length of time you keep personal data*
- *Consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;*
- *Securely delete information that is no longer needed for this purpose or these purposes; and*
- *Update, archive or securely delete information if it goes out of date*

If a patient record has not been active within 2 years of referral for original scan then our practice would be to externally archive the data, and save it for 30 years (as per NHS guidelines), disposing of any information that is superfluous such as appointment letters. The data would be stored only on digital copy off site, however we will ensure images and reports uploaded to the IEP (image exchange portal) prior to archiving.

The GDPR changes are not that dissimilar from the Data Protection principles. However the is greater emphasis on 'Data Subjects' right to be informed. The right to be informed, places greater responsibility on care providers to ensure they are communicating all pertinent information as clearly as possible and in an easy to understand way.

The GDPR - The Information commissioner's office advises:

The GDPR includes the following rights for individuals:

- *the right to be informed;*
- *the right of access;*
- *the right to rectification;*
- *the right to erasure;*
- *the right to restrict processing;*
- *the right to data portability;*
- *the right to object; and*
- *the right not to be subject to automated decision-making including profiling.*

PRINCIPLE 6:
Personal data shall be processed in accordance with the rights of data subjects under this Act.

The Data protection principles follow a similar line and as follows, are divided into clear sections:

(1) A right of access to a copy of the information comprised in their personal data (Subject Access requests):

Put plainly this means that all patients and staff members:

'…are entitled to be told whether any personal data is being processed, given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people given a copy of the information comprising the data and given details of the source of the data (where this is available)'.

Subject Access Requests need to be granted with one calendar month days of receiving a request.

The GDPR - The Information commissioner's office advises:
You should update your procedures and plan how you will handle requests to take account of the new rules:

- *In most cases you will NOT be able to charge for complying with a request.*
- *You will have a month to comply, rather than the current 40 days.*
- *You can refuse or charge for requests that are manifestly unfounded or excessive.*
- *If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.*

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

(2) A right to object to processing that is likely to cause or is causing damage or distress
The objection to processing must be written and fit the following stipulations:

- *An individual can only object to you processing their own personal data*
- *Processing an individual's personal data must be causing unwarranted and substantial damage or distress; and*
- *The objection must specify why the processing has this effect.*

The objection must be in writing the subject must stipulate why it has caused SUBSTANTIAL distress and if the service feels it is warranted cease processing for the subject. In the likelihood of it being unwarranted we must respond with written reasons why we feel it is unwarranted. Either way the subject must have a response within 21 days of the request.

(3) A right to prevent processing for direct marketing
Individuals have the right to opt out of direct marketing (using name and address, if they write stating that they want to opt out. We do not have to respond just remove them from mailing lists and 'supress' their file to ensure that no marketing continues and no future marketing can be sent in error. (In relation to HEM Clinical ultrasound this would include GP's, Midwifes, Consultants ect.. butt not patients as marketing will never be direct to patients only referrers)

(4) A right to object to decisions being taken by automated means

- *an individual can give written notice requiring you not to take any automated decisions using their personal data*
- *even if they have not given notice, an individual should be informed when such a decision has been taken*
- *an individual can ask you to reconsider a decision taken by automated means.*

Non applicable to our service as we will not be running any automated services.

(5) A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
It may be impractical to check the accuracy of personal data someone else provides. In recognition of this, the Act says that even if you are holding inaccurate personal data, you will not be considered to have breached the fourth data protection principle as long as:

- *you have accurately recorded information provided by the individual concerned, or by another individual or organisation;*
- *you have taken reasonable steps in the circumstances to ensure the accuracy of the information (see Keeping personal data accurate and up to date and Retaining personal data)*
- *if the individual has challenged the accuracy of the information, this is clear to those accessing it.*

This can be done informally where it is information such as date of birth or name spelling, but if there is a more in depth rectification needed and we are unable to comply for any reason then the subject can take the case to court.
However if there is a simple error in identification data that can be rectified the we would fill out a addendum form and attach to patients file as well as notifying the referrer if this affects the patients ongoing care directly.

(6) A right to claim compensation for damages caused by a breach of the Act.
Any individual who has been subject to a breach of data protection could claim for compensation if they can prove it has caused them emotional distress, financial damage or had an adverse effect on their physical health.
We have the right to defend our actions if we can prove we have taken every reasonable step to ensure protection against of the subject against a data breach.

The size and scope of the compensation, if we are ordered to pay it, is variable depending on the scope of the claim and the level of damage to the individual.

PRINCIPLE 7:
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This is the seventh data protection principle. In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

- *design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;*
- *be clear about who in your organisation is responsible for ensuring information security;*
- *make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well trained staff and*
- *be ready to respond to any breach of security swiftly and effectively.*

Additional guidance is in place to ensure the sufficient training of staff, on all aspects of data security by our Information security officer (Caldicott guardian). There is a clear strategy and procedure for dealing with breaches in data protection or accidental/malicious loss or damage. However, we will take all the necessary steps to ensure that the security we have around our IT assets is strong and robust.

The GDPR - The Information commissioner's office advises:
'You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach

occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself'.

PRINCIPLE 8:
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The GDPR - The Information commissioner's office advises:
If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this. The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented. This is only relevant where you carry out cross-border processing – i.e. you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states. If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.
Personal and sensitive patient information will not be sent outside of the EEA for any part of our practice so the specifications in this principle are non-applicable to our business.

DATA PROTECTION AND GDPR OVERVIEW

In short the GDPR supports the pre-existing data protection principles and expands on the following areas:

- Data Subjects rights to be informed, request information and make decisions about their information.
- Establish the lawful basis for handling data and what data specifically we hold.
- Greater accountability to firms and individuals for data breaches.
- Privacy notices must state the lawful basis for processing and what information we hold.

PRACTICAL PROCEDURES:

INFORMATION SECURITY ASSURANCE

DOCUMENT CONTROL

When considering all aspects of information security within our service, the preliminary point must be document control. By 'documents' we mean all valuable service information assets, especially confidential patient and staff information.

What are we already doing protect service users, staff and business continuity?
We have a robust document workflow in place to ensure documents are stored securely, backed up securely, and are only edited and amended by designated members of staff. We control every aspect of the information lifecycle and review policies to ensure they are relevant to the information we retain and how we retain it.

DOCUMENT LOCATION

Physical location: Hardcopy documents developed and utilised by the company and are stored in a number of secure locations:

Information Type	Where is it located?	How is it physically secure?
Patient Information	Within the clinic offices: paper copes of referrals and appointment letters are the only hardcopy patient information kept within the clinic.	All referrals are kept within the key code entry office which is always kept locked and secure day and night. With the exception of referrals in use by the clinician on the day of the clinic, these are in the possession of the Sonographer and Clinic Assistant throughout the session and returned to the offices for processing at the end of the session. All referrals are saved onto e-clinic to ensure they are backed up after the patient appointment. Appointment letters are only kept in clinic office until and posted on a daily basis. In addition the clinic is locked and security alarmed overnight.
Staff information	Within the clinic offices: Paper copies of staff information such as CV's, Training documentation and DBS checks etc... are kept within specially allocated drawers for staff.	All staff information is kept within the key code entry office which is always kept locked and secure day and night. Staff information is only removed from clinic office for staff reviews – when they will simply be taken to another room within the clinic and returned after review. Staff information is backed up digitally on management computers.
Financial records	Records such as	All Financial information is kept within the key

	invoices, Utility bills, cash flow documents etc.. are held within the clinic offices and with the company accountant.	code entry office which is always kept locked and secure day and night. Financial information is only removed from clinic office to be passed by a manager directly to the company accountant. Financial information is backed up digitally on management computers.
Patient Satisfaction Survey results	Filled in copies of the patient satisfaction surveys are anonymous, but are of great value to the company, prior to evaluation they are stored within the clinic office.	Paper copies of the surveys are kept within the key code entry office which is always kept locked and secure day and night. Once reviewed information is uploaded to our survey results document on the office computers. Paper copies are filed securely by date.
Business contracts Services and provisions database	Documentation of all business contracts are stored within the company offices in a designated file for purpose. For example – Contracted services such as IT support, E-clinic, waste management etc…	Paper copies are kept within the key code entry office which is always kept locked and secure day and night. Information is backed up digitally on company computers.
Company Policies procedures and Risk assessments	Papers copies of policies procedures and risk assessments are kept within easy access of all staff at HEM Clinical Ultrasound Service for review. These are not confidential, but are of great value to the company.	Paper copies are kept within the key code entry office which is always kept locked and secure day and night. Relevant polices and protocols are also stored in a file in the scan room which is locked at night. Information is backed up digitally on company computers. In addition copies are held on the SIRO's personal computer for documented review – so are held in triplicate for security.
Checklists for Infection control, Information governance and quality control	Papers copies of checklists are kept for review to ensure compliance. Infection control Checklists are kept within the clinic room. IG checklists and quality control checklists are kept within the clinic	Paper copies are kept within the key code entry office which is always kept locked and secure day and night. Information is backed up digitally on company computers.

	offices	

Digital Location: Key information assets are backed up digitally on the company computers to ensure retention. Patient information is stored via e-clinic on a secure cloud hosted server.

Information Type	Where is it located	How is it digitally secure?
Patient Clinical Information	On e-clinic patient management system	E-clinic provides secure cloud hosted storage for clinic patient information. Data processing agreements have been agreed and signed by both HEM and e-clinic directors The cloud storage provides storage in two locations to ensure all information is backed up should there be a server error. Access to e-clinic is monitored and specific rights given to users to carry out their role. E-clinic is has a secure gateway VPN connection, which is linked only to clinic computers.
Staff information	On Managements Computers in the company office On the Dual hard drive NAS unit.	Management computers are limited to use by managers only. Each computer is password protected. All Computers contain Anti-Virus Software and are subject to regular security scans. All the company computers are firewall protected. The room containing management computers is key code entry locked. The Clinic has security alarms which are activated overnight.
Financial records	On the Dual hard drive NAS unit.	As above. The Accountant offices have the safe physical and digital security of the clinic and are data

		protection compliant.
Patient Satisfaction Survey results	On Managements Computers in the company office	Management computers are limited to use by managers only. Each computer is password protected. All Computers contain Anti-Virus Software and are subject to regular security scans. All the company computers are firewall protected. The Room containing management computers is key code entry locked. The Clinic has security alarms which are activated overnight.
Business contracts Services and provisions database.	On the Dual hard drive NAS unit.	As above
Company Policies procedures and Risk assessments	On the Dual hard drive NAS unit. With the Company SIRO	As above Stored by SIRO securely on a password protected computer, with full anti-virus software to ensure not data loss.
Audits compiled from checklists for Infection control, Information governance and quality control	On Managements Computers in the company office On the Dual hard drive NAS unit.	Management computers are limited to use by managers only. Each computer is password protected. All Computers contain Anti-Virus Software and are subject to regular security scans. All the company computers are firewall protected. The Room containing management computers is key code entry locked. The Clinic has security alarms which are activated overnight.
Ongoing CCG and FT Billing Records	On Managements Computers in the company office On the Dual hard drive NAS	As above

	unit.	
Clinical Audits	On Managements Computers in the company office On the Dual hard drive NAS unit.	As above

PRACTICAL PROCEDURES:

NEW PROCESSES AND INFORMATION ASSETS

To ensure all information assets held within or on behalf of HEM Clinical Ultrasound Service limited are done so securely, accurately and within the law. And new processes are planned in advance by the management team and risk assessed to ensure we comply with data protection and confidentiality law. As well as our 5 question assessment procedure.

The term 'Information asset' refers to a body of information held by the company that has a productive purpose and value to the company. It is our responsibility to outline within this document what these assets are and how we conduct the processing of the information within the parameters of the law.

Information assets held within HEM Ultrasound are as follows:

- e-clinic – Patient management database
- Patient image archive on scanner
- Clinical Audits
- Results of Patient Satisfaction Questionnaire
- Hardcopy of personnel files and training
- Ongoing anonymised billing records – Swale, Medway, North Kent, West Kent
- Company financial records
- Business contracts, services and provisions database
- Company Policy, procedures and risk assessments

Due to the nature of our service the clinic operates out of a central location, this means that the information stored within the clinic is held under four conditions:

- **Software Information storage** – All computers within the clinic are kept secure behind a firewall, each computer is equipped with antivirus and antimalware software to ensure malicious code is quarantined and destroyed. With the exception of e-clinic patient management database all aforementioned software information is stored on the computers. All computers are password protected.
- **Hardcopy – paper files** – files relating to staff are kept within key code protected office room and stored within locked cabinets. Files and paperwork relating to patients are stored within a locked office room with a key code protected door, when paper data is not in use it is stored within a locked cabinet within the locked office
- **Via e-clinic –** e-clinic is the clinics online patient management system. This data is held within a secure database that can be accessed online, but is only registered to the computers within the clinic. e-clinic operates via a secure 2 x password connection database

(a vpn) and the data held within e-clinic is stored on two large software storage facilities and stored in duplicate to ensure the security and retention of data.

- **Via portable device:** These devices are 2 external storage devices and 4 USB sticks.

Information Processes:

This relates to the way in which we handle the information for each of the assets and how we ensure it is secure and of concise quality. In order to facilitate the correct recording of information each process requires a minimum dataset to ensure all the collective data is coherent and fit for purpose.

E-clinic patient management database process: Staff are equipped with a dataset with which to process all aspects of patient care on their profile which form the collective e-clinic data asset. The dataset is as follows:

- Personal contact details
- Appointment details – Type, letter, telephone confirmation
- Referral form
- Report
- Images (dicom)

Patient Images process: With regard to every scan undertaken on the scanner, each image taken is automatically saved on the scanner with the patient details attached. The scanner is not connected to the internet so is web secure and it is also password protected.
The images are transferred automatically from scanner to computer via a wireless connection which is not connected to e-clinic directly but is sent to a specially set up storage file on the computer, from there the images are uploaded manually onto the patients e clinic profile.

Clinical Audits Process: The Patients in the clinical audit are chosen at random by the IG Lead and anonymised. The Audit list is sent to Medica Reporting group – an off-site clinical auditing company, via e-mail and the Images sent via dicom transfer, directly from the scanner to Medica. The clinical audits are stored digitally and catalogued by month.

Results of Patient Satisfaction Questionnaire Process: Patients are given a questionnaire to complete within the clinic –our target is to hand them to 100% of patients, the results are collated and then displayed. The questionnaire is anonymous. The Excel sheet is held digitally within the clinic. Questionnaire results are also forwarded to referring CCG's for service patient satisfaction auditing. Results are also displayed on the monitor in the waiting room of the clinic to ensure feedback to patients.

Personnel Files and Training process – All personnel files are held within a secure locked cabinet within a key code entry office. Each employee or self-employed operator has a personnel files which contains a minimum dataset as follows:

- Staff member CV
- Advanced DBS check
- Copy of photo ID
- Performance review documents
- Mandatory Training documentation
- Any further information eg: Pay disputes and grievances etc.…

These are all held on paper form as well as scanned and backed up on the personnel computer.

Ongoing anonymised billing records – Swale, Medway, North Kent, West Kent
These are all held on excel files and require the following dataset within an excel document:

- List of referrals for each month, practices and referring clinicians within the CCG.

- List of appointments and scan types, turnaround times
- Invoice detailing quantity of scans (single/double appointments) price per scan and total

These are all saved within monthly folders per CCG.

Company financial records Processes:
All details regarding company cash flow are saved within a secure file on the management computer and are shared via secure NHS mail with the company accountant. All paperwork is stored within a locked cabinet in the Managing directors desk in a secure office. The dataset for storing financial paperwork is as follows:

Any and all financial paperwork or softcopy files to be stored regardless of current use. All purchase orders, invoices, receipts and bill's all to be stored and filed by month.

Business contracts, services and provisions list:
These are stored in paper form and digitally only within the clinic and they include, but are not exclusive to: Waste contact, fire alarm maintenance contracts, electrician contacts etc… (This is not an exhaustive list) These are filed alphabetically and stored within the clinic office and behind a door with key coded entry.

Company Policy, procedures Process:
These files are stored digitally (for review and amendments) and in hardcopy version (for easy access for clinic staff). The policy and procedures are public and are available through the company website www.hem-ultrasound.com. Company audits are undertaken in a variety of areas and include Information governance spot checks, Infection control spot checks etc… (This is not an exhaustive list)

Company risk assessments Process:
Risk assessments are stored digitally and in paper version and are held within the office behind a key code locked door. These risk assessments include information governance risk assessment, Health and safety risk assessment and Fire Risk assessment etc. (This is not an exhaustive list)

PROCEDURE FOR NEW PROCESSES:

New methods of processing information would be formulated by the senior clinic management to meet the service need. This would be discussed and approved via a meeting with the SIRO and IARO including the Operations manager and deputy. The following questions would be asked before approving any new process for information asset management.

- Will the Implementation of the process affect clinic service and Patient care?
- Will implementation of the process affect any other Information assets?
- Is the information stored securely?
- Is the information serving its purpose in the proposed form?
- Is this the best way we can utilise the information for the company needs?

Once all questions are resolved with clear and careful planning the new process can be implemented. All new processes are reviewed after one month to ensure an effective and safe processing of data assets.

PRACTICAL PROCEDURES:

NETWORK SECURITY

Due to the nature of our business it is essential that there are safeguards in place within our computer networks to ensure their security. This policy outlines what the safeguards are and how we maintain them to ensure we are compliant with our data protection responsibilities. Network security controls have been outlined by the managing director and the service director.
These controls include:

- ***Firewall***
  This is a dedicated firewall net gear security appliance, access to the internet from any of the clinic computers is only enabled through the secure firewall.
- ***Anti-virus***
  Anti-virus software has been installed on all clinic computers and is routinely updated and computers are virus scanned and document every month or when threats are detected.
- ***User access controls***
  Individual user access controls are assigned when new staff members start with the company to ensure they only have access to information required to fulfil their roll.
- ***NAS unit***
  Network attached storage allows the company to back up its most sensitive and important files separate from the internet. This allows complete security from loss due to malicious threat. The NAS unit is password protected for users, to enable access only to designated personnel
- ***Routine software updates***
  Routine software updates of applications and operating systems are essential to ensuring the smooth running of the computer systems and antivirus, as software updates include updating security settings.
- ***Secure Remote desktop connection to the patient management system.***
  E-clinic patient management system is protected via a secure gateway connection.
- ***Third party supplier contracts***
  Third party suppliers are obliged to sign a data processing agreement to ensure any data stored and controlled by them meets with our security guidelines, the data protection act and guidance from the ICO – Information commissioner's office.

Physical controls are implemented by a third party supplier. Routine checks on computers are undertaken by the same third party supplier.

PRACTICAL PROCEDURES:

SHARING INFORMATION

When sharing information for care purposes it is essential to consider whether our information sharing partners are 'trusted' organisations (having shown applicable information governance accreditation through the IG toolkit or through ISO27001 completion) or if they have not received accreditation that they comply with legal confidentiality requirements instilled on all clinical care providers.

In addition information is shared routinely with clinicians from 'trusted' care services whom have

referred patients to the service. Any clinical services responsible for a patient care, such as a GP Practice, whom may not have referred the patient (consultant referral) are in receipt of patient scan details (in addition to the referrer) providing the patient agrees to the sharing of information.

The potential hazards of not assessing information sharing partners prior to sharing information are as follows:

- Confidential information is not secure and at risk of loss
- Confidential information is not coherent and of good quality for what it is intended as there is no agreement in place for what information is shared and how the information is shared.

PROCEDURE

There are two main protocols in place for information sharing and they are as follows.

1) 'Trusted' NHS providers such as:

- North Kent CCG
- Medway CCG
- Swale CCG
- West Kent CCG
- Medway Foundation Trust
-

Are considered trusted information sharing partners as they have completed the IG toolkit, this means we are free to share information with these services without a set protocol agreed by both party's as it is complicit from completion of the IG toolkit. In addition upon completion of the AQP contract we developed a data set for information shared and a list of modes of sharing information.

Likewise we are considered a safe and secure information sharing partner due to our completion of the IG toolkit.

Other non-accredited information sharing partners such as:

- E-clinic patient management
- Medica Reporting Group limited

Are asked to sign a Data Processing agreement to ensure they comply with the company and government standards of data protection and confidentiality.

Pseudonymisation and Anonymisation for secondary purposes

All data leaving the clinic for purposes other than the patient's immediate care is anonymised utilising the patient NHS number only. This is applicable to:

- Clinical Audits undertaken by our external auditing company Medica
- Invoices to CCG's and trusts (for invoicing purposes, before sending the spreadsheet, it is run through a PAS tool to pseudonymise the data in to a code)

PRACTICAL PROCEDURES:

FAX SAFE HAVENS

These guidelines will hopefully increase awareness of some of the problems we may encounter when sending transferring/transmitting personal information and help you ensure that you have done all that you can to keep the information you wish to transmit as secure as possible.

Faxing has almost completely been phased out, we as a company have probably not received a fax in nearly a year but some surgeries do still use them so we have the following procedure in place.

It is the responsibility of all persons employed or working on behalf of HEM Clinical Ultrasound Service Limited to ensure they handle patient and staff information according to our companies policies derived from Caldicott principles and the Data protection act.

There are 4 major hazards of data movement and those are:

- Ensuring persons receiving data via fax and e-mail are receiving them in a secure location, and abiding by our polices.
- Ensuring portable devises and mediums are secure.
- Ensuring any patient or staff information is not left in a visible area where it may be seen by persons it is not intended for.
- Ensuring all staff are aware of how they handle patient and staff data and read and abide by these policies.

Procedure:

Safe Haven definition:

The term **safe haven** is term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles.

Requirements for Safe Havens:

If confidential information is received to a specific location in the Clinic:

- It should be to a room/area that is lockable or accessible via a coded key pad known only to authorised staff.
- The room/area should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to all members of staff working in the same building or office, or to visitors.
- If the room/area is on the ground floor any windows should have locks on them.
- The room/area should conform to health and safety requirements in terms of fire, flood, theft or environmental damage.

Communication by fax:

One of the most common breaches of confidentiality occurs when documents that contain patient identifiable information are sent by fax machine. Many fax machines are in corridors or open plan offices and are used by several different departments. People come and go collecting faxes but do not always check that all the pages belong to them; this increases the risk of information being seen by unauthorised persons.

To combat this, many NHS organisations have designated certain fax machines as 'Safe Haven' machines. These are machines that are located in a secure area and are used to receive documents of a private and confidential nature. If the Practice has more than one fax machine, one of them should be designated as the Safe Haven machine and should be located in a secure environment. The Practice should put policies and procedures in place for the handling of confidential information received by fax, e.g. ensuring an appropriate person is responsible for collecting and delivering any faxed information to the appropriate person.

If you are sending a fax to another organisation, ask for the Safe Haven fax machine.

No Safe Haven Fax machine?

If the organisation that you need to fax does not have a Safe Haven fax machine, then follow a few simple rules

DO …

- Telephone the recipient of the fax let them know that you are about to send a fax containing confidential information
- Ask if they will wait by the fax machine whilst you send the document
- Ask if they will acknowledge the receipt of the fax
- Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential. Please see below for a suggested form of words*.
- Check the fax number you have dialled and check again that it is correct before sending
- Request a report sheet to confirm that the transmission was O.K.
- If this fax machine is going to be used regularly, store the number in your fax machines memory.

***Suggested words for fax cover sheet**

The information contained in this fax is **STRICTLY CONFIDENTIAL** and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately.

Thank You

DO NOT…

- Send faxes to where you know that the information will not be seen for a time.
- Send faxes at times that maybe outside the recipients hours of work
- Leave information unattended whilst a fax is being transmitted

If you receive confidential information on your fax machine, it is your responsibility to inform the sender that you have received this information.

This guidance covers personal information about staff as well as patients

PRACTICAL PROCEDURES:

RECORDS MANAGEMENT AND INFORMATION LIFECYCLE

The information governance framework for the company has been developed to minimise risk of misuse of records, ensure safe data transfer and storage by assigning responsibilities for all aspects of record keeping and the management of all records including disposal to named staff with the CEO having overall accountability. All electronic data is backed up and migrated securely to ensure no data is lost due to computer malfunction, fire or other disasters on site. All data can only be accessed by authorised staff, a safe haven policy is in place to give assurance of this along with the company's business continuity framework and policy

All operational records including those for patients, staff and the company should always be complete, accurate and easily accessible but securely stored. In order to comply with this the company has procedures in place to enable all staff to effectively and accurately correlate and store information securely.

Procedure

All patient records including:

- Scan referrals
- Ultrasound scan reports
- Consent forms
- Communication between clinicians and the company related to individual patients
- Fax receipts
- Scan images

All patients' records relating to a scan appointment are held in paper format until the report has been sent back to the referrer. All are scanned onto each individual patients file held in the secure cloud based patient management system (This should be done prior to appointments and booking).

Once this has been completed all paper records are disposed of by placing into a secure confidential waste bin ready to be shredded by the company's contractor which there is a third party agreement with. All electronic patients' records should be held for a minimum of 10 years or if obstetric or pediatric – until the 25th Birthday of the data subject or unborn child.

All processes undertaken by the company are audited and regular staff meetings have a standing agenda that includes Caldicott and information governance, this was any issues can be discussed and improvements made to processes as a result of continuous audit

Staff must undergo annual IG training as part of their mandatory training so that they have a good working understanding of:

PRACTICAL PROCEDURES:

CRIMINAL RECORD DISLOSURES

All of HEM Clinical Ultrasound Service Limited's umbrella body activities. Retention periods for DBS disclosures are 2 years. It is the responsibility of the Managing Director to ensure the senior team

carry out the policy to obtain DBS certificates for all members of staff dealing with patient information or undertaking activities in direct contact with patients

PROCEDURE

- **Storage and access**
  Disclosure information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.
- **Handling**
  In accordance with Section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosure or Disclosure information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.
- **Usage**
  Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.
- **Retention**
  Once a recruitment (or other relevant) decision has been made, we do not keep Disclosure information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Disclosure information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.
- **Disposal**
  Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.
- **Utilizing subcontractors**
  Before acting as an Umbrella Body (one which countersigns applications and receives Disclosure information on behalf of other employers or recruiting organisations), we will take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of Disclosure information in full compliance with the DBS Code and in full accordance with this policy. We will also ensure that anybody or individual, at whose request applications for Disclosure are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.

PRACTICAL PROCEDURES:

SUBJECT ACCESS REQUESTS

As stated in the last chapter, patient and staff members have a right to request information regarding their care history. This is mandated by law and must be adhered to.

PROCEDURE

When receiving a data request any frontline member of staff must do the following:

- If the request is verbal, ask for a written subject access request from the patient or staff member.
- When receiving a written request pass the request to the Operations manager and/or company director.

The designated manager must then:

- Contact the patient/requesting party and ask for identification – usually confirming name, address and date of birth. Or if the requesting party is proxy for a patient due to lack of capacity- legal documents need to be supplied citing them as having power of attorney to request information.
- Discussion with clinician – who has met the patient (GP/Sonographer) regarding patients mental capacity.
- All patient data pooled from paper and digital archives to be compiled in paper/digital document – depending on the request.
- Subject to Identification confirmation patient is supplied with data requested and confirms receipt.
- All subject access requests are filed appropriately by HEM Clinical Ultrasound Service limited the following supporting evidence needs to be documented on the patient profile and annotates on the SAR spreadsheet:
    - Copy of written request for data access.
    - Confirmation of patient receipt.
    - Copy or details of data supplied.
    - Short written statement from Operations Manager/Director to state the appropriate procedure was followed in regard to the data request and was received by the patient within the correct timeframe, and patient was deemed to have capacity to receive the information without detrimental effect.

In addition the following information needs to be considered to enable the correct handling of information requests:

- Review data collection, recording and storage at the Management Meeting once per year.
- The right of access to personal data includes the right to be given a copy of the personal data.
- Employees and Patients are asked to read this information carefully and inform the organisation at the earliest opportunity if they believe that any of their personal data is inaccurate or untrue, or if they are dissatisfied with the information in that way.
- Reasonable adjustment should be made where the person making the request for access to their personal data has a disability (that for example prevents them reading the records in the form in which they are kept).
- Should Employees and Patients require access to their personal data at any time, the request must be addressed to the manager.
- The request will be judged in the light of the nature of the personal data and the frequency with which it is updated if for example a person has made a request to see their records within a short period of time after a previous request.
- If the access to the records is agreed, the information will be provided within 40 days of the date of the request. Again, you should consult the Information Commissioner's Code of Practice for guidance on any possible exemptions regarding access for personal data.
- In the event of a disagreement between an employee and the organisation regarding personal data, the matter should be taken up under the organisation’s formal grievance procedure.

- If information on any employees or Patients is requested by a third party, other than CQC, the information will not be shared unless the relevant employee or Patient has given specific written permission for the data to be released.
- Where a Patient does not have the mental capacity to be able to authorize a request to access personal data, Information Commissioner's guidance on this should be followed, that is that an attorney with authority to manage the individual's property and affairs, or a person appointed by the Court of Protection in England and Wales or the Public Guardian in Scotland to make decisions about such matters, will have the appropriate authority to make such a request on behalf of the Patient.
- The Care Quality Commission has the legal right to request and inspect any records held by the organisation in the normal course of its business. However, it is considered good practice, and demonstrates awareness of confidentiality requirements to request and obtain the permission of Patients and employees before opening their records to the Care Quality Commission. If the data subject refuses permission to the organisation to open their records, then the CQC inspector must be asked to request and obtain the data personally and directly. If the employee or patient is not present to give permission, request that the inspector look at the record of someone who is present. However, this request cannot be enforced.
- The CQC has the legal right to take copies of or remove original data and/or records from the normal place in which the records are held, with due cause. However the Provider should ensure that a written acknowledgement of the copying or removal is obtained, stating in sufficient detail of the data copied or removed.
- In the event of the death of a patient, the executor to the estate of that patient may be given access to the patient's records, if they request access and produce evidence of their status as executor.

PRACTICAL PROCEDURES:

FREEDOM OF INFORMATION REQUESTS

The Freedom of information act published in 2000 was implemented by the government to create transparency with regard to how public money is spent. The NHS is a public body and financed by the government via taxpayers. As a public body the NHS is responsible for providing information on the service to any persons whom request it. However, there are some instances where disclosure is not appropriate.
As a private company providing services on behalf of the NHS commissioners we are obligated to adhere to the Freedom of Information act 2000. This is in regard to all clinical, clerical and financial practice involved with the provision of NHS contracts.

It is essential to note that as a private company subcontracted by the NHS FOI requests regarding our service need to *ALWAYS* be handled with the help and support referring CCG's or trusts in question or passed to them directly. We are not obligated to provide information under the FOI act and would only do so to ensure our compliance on behalf of our referring CCG's and trusts.
A FOI request is not to be confused with a Subject access request, the former is related to our overall company activities and services the latter is related to individuals requesting information regarding their personal records, be it health or employee.

Please see below for guidance for subcontractors on ICO website:

'Where you subcontract public services to an external company, that company may then hold information on your behalf, depending on the type of information and your contract with them. Some

of the information held by the external company may be covered by the Act if you receive a freedom of information request. The company does not have to answer any requests for information it receives, but it would be good practice for them to forward the requests to you'.

WEB: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

In addition, there are clear guidelines for dealing with Freedom of information requests within the *NHS Standard Contract* by which we govern our service.

Excerpt from the NHS standard Contract:

Freedom of Information and Transparency
21.17 The Provider acknowledges that the Commissioners are subject to the requirements of FOIA and EIR. The Provider must assist and co-operate with each Commissioner to enable it to comply with its disclosure obligations under FOIA and EIR. The Provider agrees:

21.17.2 That this contract and any other recorded information held by the Provider on a Commissioner's behalf for the purposes of this Contract are subject to the obligations and commitments of the Commissioner under FOIA and EIR;

21.17.3 That the decision on whether any exemption under FOIA or exception under EIR applies to any information is a decision solely for the Commissioner to whom a request for information is addressed;

21.17.4 that where the Provider receives a request for information relating to the Services provided under this Contract and the Provider itself is subject to FOIA or EIR, it will liaise with the relevant Commissioner as to the contents of any response before a response to a request is issued and will promptly (and in any event within 2 Operational Days) provide a copy of the request and any response to the relevant Commissioner;

21.17.5 that where the Provider receives a request for information and the Provider is not itself subject to FOIA or as applicable EIR, it will not respond to that request (unless directed to do so by the relevant Commissioner to whom the request relates) and will promptly (and in any event within 2 Operational Days) transfer the request to the relevant Commissioner;

21.17.6 that any Commissioner, acting in accordance with the codes of practice issued and revised from time to time under both section 45 of FOIA and regulation 16 of EIR, may disclose information concerning the Provider and this Contract either without consulting with the Provider, or following consultation with the Provider and having taken its views into account; and

21.17.7 to assist the Commissioners in responding to a request for information, by processing information or environmental information (as the same are defined in FOIA or EIR) in accordance with a records management system that complies with all applicable records management recommendations and codes of conduct issued under section 46 of FOIA, and providing copies of all information requested by that Commissioner within 5 Operational Days of that request and without charge.

21.18 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of FOIA, or for which an exception applies under EIR, the content of this Contract is not Confidential Information.

21.19 Notwithstanding any other term of this Contract, the Provider consents to the publication of this Contract in its entirety (including variations), subject only to the redaction of information that is exempt from disclosure in accordance with the provisions of FOIA or for which an exception applies under EIR.

21.20 In preparing a copy of this Contract for publication under GC21.19 the Commissioners may consult with the Provider to inform decision-making regarding any redactions but the final decision in relation to the redaction of information will be at the Commissioners' absolute discretion.

21.21 The Provider must assist and cooperate with the Commissioners to enable the Commissioners to publish this Contract.

When formulating our approach to the requirements of the Freedom of information act we need to examine what elements of our service are subject to the act. This can be divided into two areas of inclusion (information covered by the act) and exclusions (information not covered with regard to our company).

Inclusions: (this list is not exhaustive)

- NHS Referral rates
- Referrals per CCG
- Volume of scan types referred
- Scan Tariffs
- Dates of contract commencement
- Outlines of service specifications for CCG and trusts
- Policies and procedures regarding the service provision.

Exclusions: (This list is not exhaustive)

- Any information with regard to private patient service activity
- Financial information with regard to our expenses to provide NHS and private services
- General Company financial information (excluding tariff paid for US procedures)
- Confidential corporate information (information that is considered sensitive and not to be disclosed for prevention of corporate sabotage)
- Any information generally acknowledged by staff members but not written down – new information should not be created to meet the needs of a FOI request.

Ultimately the commissioners, to whom the FOI is regarding, are responsible for assessing the request and asking us to provide the information to them if appropriate.

PROCEDURE:

NOTES ON COMPLIANCE WITH FOI act 2000:

- Freedom of information requests must be done so in writing, if any member of staff receives a verbal request please ask the requesting person/s to make the request in writing.
- All requests must be dealt with and responded to in full within 20 working days.
- If a FOI request is declined reason needs to be given in writing as to the reason for the rejected request.

The procedure for dealing with request is as follows:

1. Request received in writing.
2. Request passed to designated manager (Operations Manager)

3. Request reviewed for content to ensure is an appropriate request.(please see step 7)
4. Request passed to CCG or trust it relates to.
5. We receive instructions as to responding to the request or request is taken by CCG or trust for them to respond to. (if the request is taken by CCG or trust we need to inform the requestor that we have passed the request on and they will contact them directly)
6. If we are instructed to respond, information is gathered and response sent within the 20 days of receiving the request.
7. If the request is not appropriate and does not relate to any NHS service contract activity it can be rejected on these grounds. Requestor must be informed in writing. With reason for rejected request.

PRACTICAL PROCEDURES:

PASSWORD MANAGEMENT AND CLEAN DESKS

It is important for the safety and confidentiality of all service users that HEM Clinical Ultrasound Service Limited has a strong policy on password management. This policy aims to examine what is poor password management, what devices will and should have password limited access and what staff should do to ensure that confidential patient material is protected. In addition we aim to examine the benefits of a clean desk policy to ensure no patient confidential materials are left on display.

Tech equipment that staff have access to that will contain confidential patient data are as follows:

- Clinic Computers
- Ultrasound scanner
- USB sticks
- Portable hard drives

Areas where the clean desk policy applies are as follows:

- Ultrasound room
- Office
- Reception

Patient's confidential data should not be taken out of these areas, and should be filed or disposed of according to management direction.

Potential hazards of incorrect use of passwords are as follows:

- A member of staff writes down their password and it is clear for others to see their login details. This would enable staff to access information not applicable to their job, or patients are able to see the password and access sensitive information if given a chance opportunity.
- Patient information such as scan images, NHS number and dates of birth are left on the scanner and scanner is left unattended. Allowing for other staff members or patients to see confidential information without a need that is relevant. Also service users would be able to access previous scan information if left in the scan room unattended.
- USB sticks without password encryption are easily lost because of their size, and patient sensitive material could be accessed by the general public, which would be a major breach of confidentiality. This could lead to legal action and prosecution resulting in the end of the service.
- Personal passwords being given to other members of staff, this is particularly problematic as clerical audit trails would be unable pinpoint particular members of staff should there be a incident for investigation, resulting in the wrong member of staff being indicated for

investigation.

Potential hazards of not abiding by the clean desk policies are as follows:

- Confidential patient Data is left on display for members of the public to see which would be a serious breach of data protection.
- Confidential data may be seen by members of staff for whom it is not intended and not necessary for their role, which is inappropriate information to share.
- Confidential patient data may be taken by a member of the public and would constitute a major breach of patient confidentiality, and could result in legal action against the company.

PROCEDURE

In order to maintain a confidential and secure workplace protecting both staff and patients it is important that staff follow these principles**:**

- Computer passwords for individual members of staff are kept private which means: once decided on, a password is committed to memory, is not written down or saved anywhere like a phone or e-mail that may be accessed by friends and family.
- Passwords are not shared between members of staff
- Scanner passwords are only known to clinical staff and not for access of non-specified clerical staff.
- Passwords are changed every six months and are not obvious in nature i.e. 'Password' or '123456789'
- USB Sticks containing patient information are encrypted, with access only to those clinical staff who have a direct professional relationship with the patient to whom it concerns, and are always checked for security prior to leaving the premises by courier.

Clean desk procedure is as follows and should be abided by all staff at HEM Clinical Ultrasound Limited.

- Whilst not in use, or attended by staff, work areas must remain free of all patient data this includes:
- Paper copies of Patient Referral forms
- Paper copies of Reports
- Onward referral documents
- Notes from telephone conversations
- Unencrypted USB sticks
- Unencrypted discs
- Or any paperwork which contains any patient confidential data.
- In addition computer screens must not be left with windows open containing patient data that may be seen by others if unattended.

The following actions must be applied to maintain the clean desk policy:

- When not in use, but to be completed, paperwork must be placed in file boxes on each staff member's desk.
- When the paper items have been used, they must be filed away in the correct area for that patient.
- If the paperwork has reached the end of its lifecycle it must be placed in the confidential shredding bin.
- USB sticks, when not in use should not contain any personal data, and should be routinely wiped and stored.
- CD/DVR's when not in use should not contain any personal data, and should be routinely wiped and stored.
- When working on documents on the computer, if you need to leave your desk, the windows

should be minimised and the screen switched off.
- If you are leaving your desk for any length of time longer than 5 minutes you need to log off your computer so it can only be accessed again via your secure password.
- When finishing work for the day, no desks should have patient data on them and should be clear of clutter, computers should be turned off.

PRACTICAL PROCEDURES:

USE OF PORTABLE DEVISES

It has become clear in recent years that the use of portable devices within healthcare needs to be managed appropriately in order to maintain our requirements to Data protection law and to the CQC.

The following article from 2010 illustrates how complacency and incorrect procedure, being carried out by staff on USB and portable device handling, can have an adverse effect on data protection.

Dan Raywood
September 21, 2010

Unencrypted NHS USB stick lost which contained details of patients' conditions and medication

An unencrypted USB stick was lost on a train by a junior doctor after he recorded details of patients' conditions and medication in order to work from home.

The doctor from East & North Hertfordshire NHS Trust intended to hand the stick to another doctor, but accidentally took it home intending to forward the data electronically and lost the unprotected device on a train. The stick has not yet been recovered.

This has led to East & North Hertfordshire NHS Trust being found to be in breach of the Data Protection Act by the Information Commissioner's Office (ICO), whose enquiries found that the doctor had not been aware of the Trust's data protection policies and did not have access to email to receive policy reminders and updates.

The doctor informed the Trust immediately after discovering the loss and a full investigation was conducted. It was also discovered that the Trust's policies on the use of personal USB sticks were not clear and no technical measures were in place to prevent misuse of portable devices.

Article published online by SC Magazine UK
http://www.scmagazineuk.com/unencrypted-nhs-usb-stick-lost-which-contained-details-of-patients-conditions-and-medication/article/179248/

USB and portable devices are widely utilised in the workplace, and the NHS is no different. Use of portable devices facilitates ease of data transfer for many businesses and is viable for use in a healthcare workplace, as long as the risks are managed appropriately.

- All Portable devices are listed on the portable device register. This register is a complete list of all devices owned by HEM Clinical Ultrasound service Limited and utilised for clinic purposes.
- USB Sticks and Portable devices are **not allowed** to be removed from the premises without authorisation from a manager or director.
- USB sticks must be encrypted and password protected at all times whether in use or not.
- USB sticks should only be used when secure email (NHS mail) for data transfer is not an

option. If you can e-mail it securely, e-mail first, us a USB second.

- The Register of portable devices needs to be filled out daily and stored in a dated folder within the locked company offices. This also needs to be filed with copies of any forms filled out for removing devices.
- All Portable devices used are subject to regular spot checks for data protection compliance.
- All Portable devices are subject to regular checks for malware and viruses.
- Any decommissioned devises are annotated on register wiped and destroyed securely.

PRACTICAL PROCEDURES:

COMPUTER, E-MAIL AND INTERNET USAGE

HEM Clinical Ultrasound Service Limited will restrict access and use of its computer equipment, email and Internet access in order to reduce the risk of contamination of the information stored.

Where appropriate, duly authorised staff are encouraged to make use of Internet access as part of their official and professional activities. Employees of HEM Clinical Ultrasound Service Limited will have regard to their responsibility not to bring their employer into disrepute through the use of IT equipment, email or other internet based communication.

- Employees of HEM Clinical Ultrasound Service Limited will have regard to their responsibility not to breach confidentiality of their employer's information or that of their employer's clients or other employees through the use of IT equipment, email or other internet based communication.
- Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the name of the Provider or establishment.
- Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence.

Use of computer equipment

Anti-virus, Anti-Spyware and Anti-Malware.

Anti-virus software has been installed on all computer terminals within the clinic. This software has the capability to quarantine and eliminate malicious threats. It is the responsibility of the SIRO and IAO to ensure that these are regularly updated to ensure full protection. If a risk is identified the Anti-virus software will located the threat and contain it.

Contact tech support

After a virus has been discovered and contained, Staff members need to contact:

Jeff Earle – 07515 662058

jeff@eel-it.co.uk

To be assisted in removal of the virus and undertaking a full scan to ensure there is no further threat.

- The downloading of active software, in whatever format, on to the organisation's IT equipment must be authorised by the SIRO, who in turn must check that the software is safe. Be particularly wary of websites delivering active components.
- The introduction of new software must first of all be checked and authorised by the Registered Manager before general use will be permitted.
- Only authorised staff should have access to the organisation's computer equipment.

- Only authorised software may be used on any of the organisation's computer equipment.
- Only software that is used for business applications may be used.
- No software may be brought into or taken from the organisation without prior authorisation.
- Unauthorised access to the computer facility will result in disciplinary action, which may lead to dismissal.
- Unauthorised copying of data and/or removal of computer equipment/software will result in disciplinary action; such actions could lead to dismissal.

NHS Mail: Only NHS mail is allowed for e-mail of confidential patient and staff information.

The following procedure applies:

- Patient Information – such as reports/images are attached in a zipped folder to e-mails.
- Confidential information is not allowed to be written into the body of an e-mail to avoid accidental viewing by non-intended recipients.
- All NHS mail e-mails must contain an e-mail tag to include a non-disclosure request for e-mails sent in error, as follows:

'This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful. Thank you for your co-operation'.

- No member of staff is allowed to share their NHS mail password with another member of staff.
- All e-mails are archived for auditing purposes.

USE OF PERSONAL E-MAIL

- HEM Clinical Ultrasound Service Limited will not tolerate the use of -mail at work for unofficial or inappropriate purposes, including:
    - Any messages that could constitute bullying, harassment or other detriment;
    - Accessing or transmitting pornography;
    - Personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
    - Online gambling;
    - Social networking;
    - Transmitting copyright information and/or any software available to the user;
    - Posting confidential information about other employees, the employer or its customers or suppliers.
- In addition staff members are prohibited from downloading any documents or programs if they do not firstly have permission of the SIRO and secondly are absolutely sure they know the source.

Use of web browsers

- Web browsing is made available for research purposes only, and use of the organisation's IT equipment for browsing for personal purposes is permitted only permitted during lunch hours and breaks.
- Only websites known to be reputable may be accessed using the organisation's IT equipment,

in order to protect the equipment from malicious intrusion. The user must take personal responsibility for determining if the site to be accessed is safe, and failure to take reasonable precautions may result in disciplinary action.

- The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the internet to access and/or distribute any kind of offensive material, or matters not related to the employer's business, will render the individual liable to disciplinary action which could lead to dismissal.

PRACTICAL PROCEDURES:

MOBILE WORKING

The needs of the business may sometime require that members of staff work from an office outside of the clinic, and or from home. When this need arises it is important for the company to place working procedures in place to ensure the following standards are met:

- No patient or staff private and confidential information is removed from the business premises on a portable devise or laptop unless done with the express permission of a senior manager, and is necessary for the individual to complete their work.
- If a portable device is used it must be password protected and encrypted.
- If a laptop or personal computer is used it must equipped with up to date anti-virus software to the company standards (Please see Information security breach policy and procedure version 1.0).
- The member of staff must be sure they abide by the company health and safety policy to ensure their working environment meets the essential standards of health and safety.
- They abide by the Companies Clean Desk Policy (Version 1.0) to ensure that they do not leave any sensitive information on computer screens where it can be viewed by anyone.

Physical Security:
Transporting information: Information is at high risk of loss or theft during transportation. It is important that mobile workers ensure they do not leave any portable information unattended or without locked protection.
Home: Mobile workers ensure they take in to consideration physical security of data when working from home. Mobile workers must be sure to assess the risks of theft at home and take appropriate steps – door security, alarms etc.

PRACTICAL PROCEDURES:

DATA QUALITY

As a company working with the NHS we are reliant on the continual supply of patient information from GP's and Consultants to create our patient profiles. The patient referral form acts as a legal document validating the patient's referral to our service. The information contained within each patient referral should meet the minimum standards for us to complete our role as a supporting service to primary care.

It is important for patient care to ensure the data we receive is transcribed accurately and completely when creating patient profiles and throughout the patients care pathway with us. Due to the formative nature of our company we are heavily reliant on data entry by individual users, and as such can be subject to errors and omissions due to the human element.

We have a legal commitment to our AQP contract particulars and we must complete and annual

submission to the IG toolkit (an online portal for Information governance compliance). A large part of our IG compliance is Information quality and retention, as such the company's attention to information quality need to be of a high standard.

PROCEDURE

Referral forms are the first and only document received from the GP to initiate the scan appointment. Patient information available on the referral and subsequently entered into the patient profile are as follows:

- Full Name
- Date of Birth
- NHS number
- Gender
- Address
- Contact Telephone Number
- Disabilities which may affect the scan
- Scan requested (Eg: Abdo & Pelvis etc..)
- Clinical Indication
- Surgery name
- GP name
- GP code
- Surgery Code
- Date of referral

All this information needs to be entered into the patient profile verbatim from the referral form.
In addition, the referral form must be attached to the patient profile in a viewable PDF format, when the patient profile has been created. The Patient referral must be annotated to state the date when the referral was received and **NOT** the date the referral was attached to the patient profile.

ONGOING RECORDED DATA

The following entries need to be completed into every patient profile to ensure fidelity of patient information:

- All communication – including letters and phone calls - time stamped
- Patient notes – containing all pertinent information relating to patient care not found in communications. Scan type, preparation, notes from communications – Time stamped
- Treatment and appointment records and DNA's – time stamped.
- Reports – cross referenced with relevant referral and images
- Patient consent form
- Patient Images
- Fax confirmation sheets attached

CROSS REFERENCING

Reports need to be annotated by the reporting sonographer and assistant to indicate the referral applicable to the scan. This is done through the clinical indication. For example:

- Referrals archived in attachment as ' Referral received '06/10/2016'
- Clinical indication on report 'Clinical indication: C/O vague abdominal pain but more especially around renal angle bilaterally? Cause (from referral received 06/10/2016)'
- Images need to be recorded titled as 'Images from report 11/10/2016'

As we received multiple requests for the same patient it is essential for clinical auditing purposes we identify the correct referral in the body of the report and are able to cross reference with an attachment of the same title.

PRACTICAL PROCEDURES:

DATA ENTRY ERRORS

The company is responsible for ensuring that all data generated by the company is accurate and appropriate. That the company complies with all data regulations that are relevant to the service the company provides. In the case of a data error there must be systems in place to ensure that all errors are investigated using the company's root cause analysis process.
In the case of minor incidents a report must be filed and kept in the company's incident file, along with any remedial action taken and follow-up audits completed to monitor any improvement plans established as a result of an incident, so that the company can be assured that the remedial action has reduced the risk of recurrence.

For more serious data errors, including 'never events', for example errors that may result in incorrect patient data being placed onto the wrong patient files such as a diagnostic report, a more robust root cause analysis investigation must be carried out in these circumstances and the patient and or referrers must be informed immediately with analysis of the level of severity, these types of data errors have the potential to become clinical errors which may impact on patient care, therefore the process will move from a data error investigation to a clinical SUI investigation.

PROCEDURE
HEM Clinical Ultrasound will investigate all minor and serious incidents concerning information governance issues to ensure that lessons are learnt and the risk of reoccurrence is minimised.
The process for investigation

- Scoping
- Assessing grade
- Initial reporting
- Managing the incident
- Investigating
- Final reporting and lessons learnt

Definition of a Serious Untoward Incident in relation to Personal Identifiable Data
Department of Health[1] guidance explains that there is no simple definition of a serious incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa.
As a guide, any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious.

Please see Practical Procedure - Data Security Breaches

Minor Errors
Minor errors and omissions of data need to identified and added to the operations manager's errors log. Minor data errors identified by third parties such as commissioners, GPs, Patients and non-HEM clerical staff need to be documented in the applicable patient profile and errors log. The error needs to be rectified be the designated staff member and the third party must be notified in writing of the

rectification. All communications must be included in the errors and omissions log for data continuity.

Reporting to external bodies

1) If a SUI is classified as level 0 then the Company may manage this locally and there is no requirement to report externally.
2) If the SUI is classified as level 1-5 then the Company will report the SUI to the relevant CCG in line with the SUI reporting policy
3) If the SUI is classified as level 3-5 then the Company will also report to the Information Commissioner.

The decision to inform any other bodies will also be taken, dependent upon the circumstances of the incident, e.g. where this involves risks to the personal safety of patients, the National Patient Safety Agency (NPSA) may also need to be informed.

Informing Patients

Consideration should always be given to informing patients when person identifiable information about them has been lost or inappropriately placed in the public domain. Where there is any risk of identity theft it is strongly recommended that this done.

Root Cause Analysis

A root cause analysis investigation needs to be carried out to establish the cause of the incident and to create a practical plan to implement change to reduce/eliminate the risk of reoccurrence.

PRACTICAL PROCEDURES:

SERIOUS UNTOWARD INCIDENTS – IG

A serious incident is an occurrence that results in either a near miss of harm to a patient or results in harm to a patient. The range and type of referrals for non-obstetric diagnostic scans we can accept as part of our NHS contracts means that the risk of finding a serious pathology is statistically low, however serious unexpected pathology is occasionally found whilst a scan is being performed and along with the potential for finding an unexpected pathology is the risk that a pathology may be missed, this is also the case for all private non-obstetric scans. The potential for a missed pathology or a miss diagnosed pathology is always a factor to be considered and the risk mitigated by high standards of clinical practice and continued clinical audit along with continued professional development for all clinicians employed by the company.

The other potential clinical risk associated with the companies type of diagnostic service is that of a clerical error, a clerical error also has the potential to cause a serious clinical incident, examples of significant clerical error are:

- A normal report put on the wrong patient's profile and sent back to the referrer
- A report escalated in error for the wrong patient due to being put on the wrong patient's profile

The two potential errors listed above have the potential to impact on two patients; the patient whose report was placed on the wrong patient's profile & the patients whose profile was wrongly used.
All serious clinical errors must be investigated and reported to the Care Quality Commission (CQC) all

near misses have also to be investigated and in both cases the company must carry out a full Route Cause Analysis (RCA) into the cause of the incident and the outcome of the RCA must offer a strategy for improvement and monitoring of improvements implemented to assure and insure that the risk is reduced of a similar incident happening again.

PROCEDURE

Minimise risk of Clinical error risks

The risk of clinical errors is minimised by:

- High standards of clinical practice
- Continued clinical audit
- CPD
- Only working within the individual clinician's scope of practice
- Always check that the patient's details both on the scanner and on e-clinical reporting system match the patient you are scanning and reporting on

In addition we ensure that:

- All clinical staff employed by the company must have a minimum of 5 years' clinical practice experience
- Be state registered
- Be DBS checked
- Have proven CPD
- Continued clinical Audit; 5% of all scans and reports performed by practitioners are audited each month by specialist Radiologists to assess image quality and accuracy of reports
- CPD continued professional development must be shown for all clinicians, this includes self-development via reading medical articles and attending relevant courses
- All clinicians must know their professional limitations and only practice within their individual scope of practice, i.e. never attempt scans that they are not competent to perform
- Prior to each scan the clinician performing the scan must check that the patient demographics on the scanner match the patient being scanned, further when reporting on e-clinic always check that the patient profile matches the patient you are reporting

The risk of a missed diagnosis or a miss-diagnosis is minimised if all the above is followed.

Minimise risk of Clerical error

The minimising of clinical/clerical risk starts with the referral being sent to the company by a referring clinician:

- **Stage one** triage of the request by a clinician; does the clinical indication match the type of scan being requested? if it does then the correct patient preparation must always be documented
- **Stage two** the clerical team must upload the patient's referral onto the correct patient profile or create a new patient profile with the correct patient demographics if a new patient
- **Stage three** the patient is contacted either via letter or a phone call, identity must be checked if a phone call or correct demographics used if a letter is sent
- **Stage four** When the patient arrives for the scan the receptionist must check patients name and ask them to complete a consent form
- **Stage five** the patient is called into the scan room by the clinic assistant who checks the patients name, date of birth and first line of address with the patient
- **Stage 6** The clinician performing the scan must always double check the patient's details are correct on both the scanner and the e-clinic profile prior to doing the scan and writing the

report
- **Stage 7** clerical team sending the completed report back to the referrer must double check the content of the report against the referral criteria i.e. renal report matches renal referral, prior to sending the report back to the referrer

If all these stages are completed routinely then the risk of a report being placed on the wrong patient's profile and or the wrong report being sent back to referrer is minimised.

PRACTICAL PROCEDURES:

DATA SECURITY BREACHES

To meet the seventh data protection principle of the Information Commissioner's Office (ICO), which is:

> *"Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

In addition we will look at the chain of accountability in light of the new EU legislation the General Data Protection Regulations.

HEM Clinical Ultrasound Service Limited, as an organization which processes personal data, must take appropriate measures against unauthorized or unlawful processing and against accidental loss, destruction of or damage to personal data.

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorized use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organization who holds it.

We are taking account of all data relating to HEM Clinical Ultrasound Service Limited, its patients and employees held within the organization or its associates, however stored. We want out a clear agenda for dealing with data security breaches and is set out as follows:

- Assessing the risks
- Containment and recovery
- Who and when to notify of a breach
- Evaluation & response
- Safeguarding for the future

PROCEDURE

If breach has occurred, there are four important elements to any breach management plan:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.

•Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
•Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of backup media to restore lost or damaged data or ensuring that staff recognize when someone tries to use stolen data to access accounts.
•Where appropriate, inform the police.

Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of an employee database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary, further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of

financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification of breaches

Informing people and organizations that you have experienced a data security breach can be an important element in your breach management strategy. However, informing people about a breach is not an end in itself.

Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

From 26 May 2011 certain organisations (service providers) have a requirement to notify the Information Commissioner (ICO), and in some cases individuals themselves, of personal data security breaches.

Assessing the Severity of the Incident

The immediate response to the incident and the escalation process for reporting and investigating this will vary according to the severity of the incident.
Once we have determined that the incident is serious we should then grade the incident according to the following table; an incident should be categorised at the highest level that applies when considering the characteristics and risks of the incident.

0	1	2	3	4	5
No significant reflection on any individual or body Media interest very unlikely	Damage to an individual's reputation. Possible media interest, e.g. celebrity involved	Damage to a team's reputation. Some local media interest that may not go public	Damage to a services reputation/ Low key local media coverage.	Damage to an organisation's reputation/ Local media coverage.	Damage to NHS reputation/ National media coverage.
Minor breach of confidentiality. Only a single individual affected	Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted	Serious potential breach & risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected	Serious breach of confidentiality e.g. up to 100 people affected	Serious breach with either particular sensitivity e.g. sexual health details, or up to 1000 people affected	Serious breach with potential for ID theft or over 1000 people affected

Answering the following questions will assist other types of organisations in deciding whether to notify:

•Are there any legal or contractual requirements? Service providers have an obligation to notify the Commissioner in certain circumstances. Health and Social Care providers will have a legal responsibility to notify their Regulator of breaches, and may have a contractual obligation to notify commissioners of services, such as Social Services or NHS.
•Can notification help you meet your security obligations with regard to the seventh data protection principle? This is "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."
•Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
•If a large number of people are affected, or there are very serious consequences, you should inform the ICO.
•Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

- Have you considered the dangers of 'over notifying'. Not every incident will warrant notification and notifying a whole customer base of an issue affecting only one customer may well cause disproportionate enquiries and work.

You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to your decision:

•Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notify them of any type of breach but the ICO should only be notified when the breach involves personal data
•There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation

- Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach

•When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them
•Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

•When notifying the ICO you should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred. You should also inform us if the media are aware of the breach so that we can manage any increase in enquiries from the public. When informing the media, it is useful to inform them whether you have contacted the ICO and what action is being taken. ICO will not normally tell the media or other third parties about a breach notified to us, but we may advise you to do so.
The ICO has produced guidance for organisations on the information we expect to receive as part of a breach notification and on what organisations can expect from us on receipt of their notification.

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and outline responsibility in the light of experience.

You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.

The following points will assist you:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved. Your notification with the Information Commissioner will be a useful starting point.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do you store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether you need to establish a group of technical and nontechnical staff who discuss 'what if' scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions
- If you have completed the Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches, or incorporating security breaches into the overall Business Continuity Plan. Breach of data security could in some circumstances be serious enough to endanger the business.
- It is recommended that at the very least you identify a group of people responsible for reacting to reported breaches of security**.**

ICO INFORMATION SECURITY BREACH NOTIFICATION FORM

ico.
Information Commissioner's Office

Security breach notification form

This form is for data controllers to report a breach of security to the ICO. It should take about five minutes to complete.

Before completing this form, you should read the following guidance: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant information, e.g. incident reports.

Sending this form

Send your completed form to casework@ico.gsi.gov.uk, with 'Security breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- A case reference number; and
- An explanation of what to expect during our investigation of the incident.

If you need any help in completing this form, please contact our helpline on

0303 123 1113 or **01625 545745** (operates 9am and 5pm Monday to Friday).

Security breach notification form

1	What is the name of your organisation (the data controller)?	
2	Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)	
3	Have you notified as a data controller? If so please provide your registration number. Search the online Data Protection Public Register.	
4	Have you reported any previous incidents to the ICO? If so, please provide brief details and reference numbers, where known.	
5	When did this incident occur?	
6	Please briefly describe the incident.	
7	Has any personal data been placed at risk? If so, please give us an outline of what this data consists of.	
8	Approximately how many data subjects have been affected?	
9	Have you informed the data subjects that this incident has occurred?	
10	Has there been any media coverage of the incident?	

11	Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so please provide brief details.	
12	Are you carrying out an investigation into the incident - If so when will you complete it and what format will it take?	
13	Have you informed any other regulatory body of the matter? If so please provide their details and an outline of their response.	
14	What action have you taken to prevent similar incidents in the future?	
15	Is there any other information you feel would be helpful to the ICO's assessment of this incident?	

PRACTICAL PROCEDURES:

DATA PROCESSING AGREEMENTS

All companies contracted to carry out work using confidential information on behalf of HEM ultrasound are obligated to sign a third party data processing agreement. The Data processing agreement is even more pertinent to Information governance operations following the implementation of the GDPR (General Data Protection Regulations) from May 2018.

The data processing agreement ensures the following GDPR compliant safeguards when dealing with confidential information on our behalf:

It is the responsibility of the managing director to ensure there are safeguards implemented; it is then the responsibility of the designated manager responsible for subcontracting to ensure the agreement is signed and in place prior to information exchange, and that the agreement is reviewed annually for change in legislation and best practice guidance.

The purpose of the data processing agreement is to ensure that hazards are mitigated and both parties are mindful of their responsibilities to the agreement. Potential hazards such as data breach and loss are covered by the Data processing agreement – specifically liability under the circumstances.

Prior to implementing the third party agreement the company needs to carry out a data privacy impact assessment on the third party provider. This process is started by asking the following questions:

Our Service requirements:

1. What type of data will need processing? Is it classified as 'personal data', 'sensitive personal data' or 'commercially sensitive data'. Each data type requires a different category of risk assessment.
2. How will the data be processed?
3. What quantity of data will be processed?

After establishing responses to these questions a data protection impact assessment needs to be completed please see below example of impact assessment as required by the GDPR.

Data Privacy Impact Assessment

What is the processing Activity (Describe in detail the processing activity to be carried out on behalf of HEM Clinical Ultrasound Service LTD.	LEVEL OF RISK

What are the hazards?	Who might be harmed and how?	What are you already doing?	Do you need to do anything else to control this risk?	Action by who?	Action by when?	Done

From completion of the Data Privacy Impact assessment there will be clear areas for action and improvement prior to May 2018. These areas for improvement will be implemented and agreed following the annual revision of the data processing agreements. Further action may be needed should controls not be sufficient.

The Data Processing agreement:

The Data processing agreement sets out the relationship between the 'Data Controller' (HEM) and the 'Data Processor' (e-clinic). The data processor must abide by the agreement with respect to the 'purpose' of the data processing and ensure they operate according to the law (GDPR and DPA) and stipulations made within any additional clause