Mid Essex Hospital Services NHS Trust

Information Governance Handbook

For All Permanent Staff, Locums, Temporary Staff, FED Staff, Agency Staff, Contractors, those on Work Experience and Volunteers

Version 2.0
July 2011

Dear Colleague

I am pleased to provide you with your own copy of the Information Governance Handbook. You have received this with your payslip as it as it is the one way we can guarantee to our auditors that you have been informed of and have ready access to your key information governance responsibilities and that you are aware of how to manage patient and trust information safely and securely.

Information Governance concerns all aspects of how the NHS handles information about patients, staff and its corporate affairs. Trust staff create, access, transfer and modify sensitive information every day and it is vital that it is managed legally, securely, efficiently and effectively. Failure to do so can involve the trust in heavy fines, but most importantly, lead to a lack of trust by patients and a lot of unnecessary negative media interest as well as the possibility of disciplinary action for the staff responsible.

There are a large number of policies that come under the umbrella of information governance and this document includes a full list, but we have decided that it would be helpful to bring together all the important messages from all these policies into one place for you.

Please take some time to read this document and then keep it close by as a useful reference.

We know we will!

Yours sincerely

Malcolm Stamp	**Matt Bushell**
Chief Executive	**Director of Business Development & Performance and SIRO (Senior Information Risk Owner)**

Index

1. Introduction

Staff must be aware of the Trust's expectations of them for work practices and behaviours relating to Information Governance. Specifically staff must be aware of:

- all the policies and procedures that pertain particularly in relation to confidentiality, information security, data quality and the general day to day protection of sensitive information
- how to access the policies and procedures
- what training must be undertaken
- the trust's procedure for managing Subject Access Requests (SARs)
- responsibility for clinical record keeping and generally observing all medical records procedures, including casenote tracking and timely and correct filing
- their responsibility to access confidential information on a demonstrable "need to know" basis
- the necessary arrangements for sharing information with others
- the fact that monitoring and auditing of access to confidential information is carried out
- evidence of failure to comply with any of the above may result in formal disciplinary action, up to and including dismissal

Trust policies and procedures are all based on legal and NHS frameworks which include:

- The Data Protection Act 1998 which applies to any person who has access to or handles information. The 8 Principles of this Act govern how personal identifiable information is gathered, stored, accessed and released.
- Confidentiality NHS Code of Practice – provides guidance to the NHS on patient information, confidentiality and consent
- Caldicott Principles – 6 Principles governing appropriate management of specifically patient information (overseen locally by the Caldicott Guardian – each Trust must have one)
- Records Management NHS Code of Practice – this code is a guide to the required standards of practice in the management of records and includes creation, naming, storage, access and retrieval of all records. All staff are responsible for any records they create or use during their daily duties
- Information Sharing: Guidance for Practitioners and Managers
- The Information Governance Toolkit – the trust to be able to demonstrate that we have the appropriate evidence against 43 individual criteria that we manage all our information safely and appropriately – the results are audited and also feed into the Care Quality Commission Outcome 32

2. Policies

The Trust has a range of policies that come under the heading of "Information Governance" . These are all published on the intranet and on the external website and the easy way to find them is to put the unique trust register number into the search engine and only that document will appear. There are a lot of documents so the ones that you are most likely to need to reference are in bold blue. Documents that are specific to IT internally such as "Network Security" are not included.

Register No	Name	What's it about?
07012	Information Governance Strategy	This is the overarching policy under which all other policies refer. This document will tell you the direction of the trust but not give specific task guidance
09045	Information Security Management Strategy	This is the overarching policy under which all IT security and IT specific policies refer. This document will tell you the direction of the trust but not give specific task guidance
04084	Records Management Strategy	This is the overarching policy under which all records related policies and procedures refer. This document will tell you the direction of the trust but not give specific task guidance.

07011	**Confidentiality Policy**	**This is the key document that relates to all aspects of confidentiality**
06019	Data Protection Policy	Relates purely to how the trust will meet its obligations under the Data Protection Act
07026	**Sharing Patient Information**	**Key document that sets out the rules for sharing patient information outside the trust and a Data Sharing Agreement is appendixed**
08088	**Acceptable Use of IT**	**This is the key document that relates to safe computer usage**
08075	Workstation Security	How to work safely at your computer
09036	Password Policy	Management of passwords
07042	Email Policy	Staff responsibilities about the use of email
08064	Encryption Policy	All mobile media must be encrypted including laptops, memory sticks. Trust information can only leave the trust on media that is encrypted
09021	Remote Working	Rules for secure working with IT for staff who are either mobile or working outside of the trust eg at home
10055	Sending Patient Identifiable information out of the UK	This policy relates specifically to the Data Protection Act and its Principles and the policy sets out the rules for managing this in the trust
09035	Paper & Electronic Waste Policy	The rules for confidential destruction
08042	**Document Provenance Policy**	**This sets out the rules and standards for all trust policies, clinical and non-clinical**
08022	Information Lifecycle Policy	The Trust's first policy relating to trust records management
10123	Information Asset Policy	Sets out the responsibilities of Information Asset Owners and Information Asset Administrators to the SIRO for the correct recording of information assets onto the trust database
04085	Archiving Policy	Relates mainly to the archiving of Medical Records – staff must also need to know about the **Retention & Disposal** schedule that sets out the rules for how long trust documents needs to be retained
04086	**Access to Records Policy**	**The rules and procedures for meeting DPA Subject Access Requests and requests from other agencies including the Police for duplicate health records**
07015	Coding Policy	The management of medical coding
08086	**Clinical Record Keeping**	**The required procedures for clinical record keeping**
05103	Casenote Tracking Policy	The rules concerning the tracking of medical records and specifically how each movement of each record must be recorded on PAS
06019	Data Quality Policy	The trust policy for achieving data quality relating to patient activity
09031	Registration Authority	The rules around smartcards
07014	Freedom of Information	Reflects the FOI Act and includes the trust process for the appropriate management of the Freedom of Information requests it receives

There are associated policies that do not come under the heading of Information Governance but have substantial information governance content that particularly relates to the "secondary uses of data", appropriate access to health records, information risk and IG Serious Untoward Incidents

- 08076 Clinical Audit Strategy
- 08042 Research & Development Policy
- 09100 Incident Policy
- 04061 Risk Management Strategy

3. Confidentiality – Best Practice Guidelines – In Brief

There is now absolutely no public acceptance of breaches or confidentiality or data loss and in the event of being found guilty of "reckless loss of data", the Information Commissioners Office (ICO) are empowered to levy fines of up to £500,000 on negligent organisations. Any breach of confidentiality is an automatic Information Governance Serious Untoward Incident (SUI) which is measured on a scale of 0-5. Any incident that qualifies as a Level 3 or above must be reported to the ICO. As an example of a SUI that would be recorded as a Level 3, would be medical or nursing handover sheets totalling more than 20 patients, found outside the hospital grounds. The public are now far more likely than in the past, to publicise any breach event to the local or national media, because of the risk of identity fraud and also to demonstrate the unacceptability of carelessness or thoughtless actions of trust staff. Media interest alone can drive a Level 1 or 2 SUI to Level 3 or above.

Confidentiality requires staff to maintain patient and trust information safely. This requires a variety of procedures to be followed at all times, specifically:

3.1 Conversations

- when in a clinical area or anywhere where you can be overheard by other patients, visitors or non-associated staff, do not talk about patients by name, this applies in face to face situations and on the telephone
- When speaking on the Vocera system not only may people around you hear what you are saying but so may others who are in the vicinity of the person you are speaking to – it operates like a hands free mobile phone – **users must be careful** – check your environment and that of the person you are calling before naming a patient or sharing confidential information
- if you see someone who you recognise and you are on a path or corridor, in a waiting area or in the restaurant, and you were unaware that they were coming to hospital, do not approach them – if they recognise you and stop you or call out, then it is alright to speak to them – but do not ask them why they are here – they may not want to tell you and you could be putting them in an embarrassing situation

3.2 Telephones

- make sure you cant be overheard discussing person identifiable information
- if someone rings and asks for personal information, be absolutely sure that they are who they say they are and they have an entitlement to the information
- if someone calls from a business or company, take a message and make sure that you take down the company switchboard number, not an extension or mobile phone number
- Provide the information to the person who asked for it, don't leave messages
- if in doubt at all, ask your manager or Information Governance Manager
- get patient consent to leave a message on a landline – actually its better to text a mobile

3.3 Email

- do not send patient identifiable or other sensitive information out of the trust using an nhs.uk email address unless it is encrypted. It is not secure
- if you are regularly needing to share patient identifiable or other sensitive information with other nhs colleagues, set up a secure nhs.net account by logging on to www.nhs.net
- if you are regularly needing to share information with other central or local governmental non-nhs colleagues eg Social Services, they should be able to provide you with an equally secure email address to send to eg .gsi or .cjsm . If they say they have no such capacity, then regretfully you will not be able to send the information. They **will have the capacity** as they are all part of the "Secure PAN-Government Network". If this becomes a problem, contact the Information Governance Manager who will contact the body on your behalf

3.4 Faxing

Faxing is the **least** favourable method of communication. The possibility of mis-keying in numbers and the faxes then being received by a member of the public or non-associated business is very high. If you absolutely must fax then please follow these rules:

- check whether you really need to fax it!
- could you exclude the patient identifiable element or anonymise it eg by using just hospital number and exchanging the hospital number for the name over the phone?
- If not – telephone before you send it and ask for a confirmation call when received
- If this isn't practical because of the quantity of faxing to be done, pre-record as many fax numbers as possible into the fax machine – this will reduce the opportunity for misfaxing
- Make sure the fax cover sheet states who the information is for and mark it "Private & Confidential"
- Request a report sheet to confirm the transmission and number it went to.

3.5 Portable Media

The requirement to have encryption in place is absolute. Using unencrypted portable media for transporting confidential information out of the trust is the information governance example of a "never event". Portable media includes laptops, CDRoms and USB sticks but also means any device at all that could potentially be used for downloading. The rules are:

- do not download any sensitive information onto any portable device unless it has been encrypted even if the device is never leaving the hospital grounds – it can still be subject to theft
- do not use USB sticks as sources of permanent storage – they have no other purpose than for safe transportation
- if you need to download and take information off site and you do not have a trust issued device, you may ask IT Helpdesk to encrypt your own USB stick
- make sure you have permission to download or take any trust information out of the trust even if it is encrypted
- all portable media must be locked up whilst not in use
- never leave the password to the encryption of the device in the on or near the device – it renders the whole process of encryption pointless

3.6 Postal Services

Ideally, all posted communications that include patient identifiable information should be sent by recorded/registered mail, however that is not practical or affordable, therefore trust staff need to mitigate this risk by:

- marking envelopes as Addressee Only, Private & Confidential
- ensuring that the trust name is not franked on it
- making sure that envelopes are sealed
- Large envelopes or packages eg copies of medical records are sent in tamper proof envelopes eg Tyvek Anti-Tear or heavy duty bubble wrap or similar envelopes

3.7 Sending Patient Information out of the UK

This matter is very specialised and few staff are involved. Anyone who is must refer to the specific Trust policy number 10055. Any issues not resolved by referral to the policy must be forwarded to the Information Governance Manager before the information is sent.

What is key is that if patients asked for their information to be sent to a country outside the Economic Union, they need to be aware that we cannot guarantee the safety and security of their information, either manual or electronic, and they must consent in writing to accept the risk, before we send it.

3.8 Disposal of Confidential Information

Policy 09035 Disposal of Paper & Electronic Waste covers this. The basic rules are:

- all confidential information must be disposed of in a green postal type confidential waste bin or shredded by a cross-cut shredder. A straight line shredder is not acceptable for this purpose
- do not use any paper with confidential information on it as scrap paper
- do not try to save money by printing information on the back when the front has been used for patient identifiable information that is no longer required eg old clinic lists

- do not put any IT equipment in bins or skips – it must all be collected by the IT department for appropriate disposal or wiping
- if there is bulk disposal required and there are insufficient green bins, it is possible to use the white sacks as long as:
    - they are in good condition with no holes or tears
    - you have single use cable ties to secure them
    - you only fill them two-thirds full
    - you ask the porters to remove them as soon as they are sealed
    - they are never left around open

3.9. You, Your Workstation, Work Area or Desk

- wear your identity badge at all times
- be aware of "tailgaters" when opening swipe doors – do you know who they are?
- politely challenge anyone who appears to be accessing information that you don't think they are entitled to see
- lock up everything sensitive when leaving the area unmanned, don't leave sensitive information lying around on desktops
- don't let anyone (particularly patients and visitors) see what is on your computer screen
- don't permit patient identifiable information on whiteboards
- keep your password confidential at all times and share it with no-one
- log off when you are not at your desk
- don't allow anyone to access networked services whilst you are logged on – you then become responsible for what they access which maybe inappropriate and a breach of policy and maybe subject to disciplinary action
- use a strong password – with lower case, upper case and numbers
- never keep passwords adjacent to the device to which it refers eg writing the encryption password on the back of an encrypted data stick or, on a post-it note on the wall
- complete a risk event form for all perceived breaches of confidentiality however minor you believe them to be
- put whatever sensitive information you no longer need to keep, in the confidential waste bin or delete it from your electronic files – but refer first to the Retention & Destruction Schedule on the intranet as most documents created by the NHS have a minimum retention period some of which reflect legal frameworks
- don't print anything you don't absolutely have to

4. Maintaining Electronic Security

A number of measures have already been referred to in the Confidentiality section above but staff must also:

- use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs or Trojan horse code
- not forward on "junk email" – you are contributing to email "spam" – this includes forwarding chain letters or pyramid schemes
- remember that if they contribute to newsgroups on the internet using a Trust email address then the posting should contain a disclaimer stating that the opinions expressed are their own and not necessarily those of MEHT (unless posting is in the course of business duties)
- know that limited access to the internet for personal purposes is permitted and this should preferably take place out of normal working hours and must not interfere with the works that the staff are contracted to carry out
- be aware that usage of the internet is closely monitored on a daily basis and the monitoring includes:
    - the amount of time spent overall
    - the types of sites visited
    - any inappropriate search criteria
- not engage in deliberate accessing of offensive, obscene or indecent material from the internet such as pornography, racist or sexist material, violent images or incitement to criminal behaviour

- if the web filter indicates that the internet site(s) that staff want to visit are "blocked", staff must accept this and not make any effort to circumvent this control eg by attempting to use proxy websites. Staff found to be attempting to access proxy web sites will be subject to disciplinary procedures
- all staff who are teleworking or using mobile computing must follow the guidelines provided

5. Registration Authority – the Use of Smartcards

All doctors and some nursing and administrative staff are issued with Smartcards that provide access to patient information on the national Summary Care Record including the Choose and Book system.

The card is not specific to MEHT and is portable, so if a card has been issued to you at another hospital, they will have cancelled the access arrangements there before you left and once you start work here, MEHT will allocate the appropriate accesses you need here onto the same card.

Smartcards are extremely important and must be protected. You must give them the same respect you would your credit cards. There is detailed information about trust Registration arrangements in 09031 Registration Authority Policy but in brief, staff must be aware of the following:

- that Smartcard usage is monitored and if the rules are breached, the cardholder may be subject to disciplinary procedures
- it is the responsibility of each Smartcard holder to be aware of the current terms and conditions - each holder is provided with the terms and conditions at the time a new card is issued but these are updated regularly and staff must read the updates as these are issued
- if a Smartcard is lost, the holder must notify the Registration Authority office in the HR Department **immediately** so that the card can be electronically cancelled
- do not leave Smartcards in computers and leave the area – remember to take your card with you or someone else may use your access
- never use someone else's smartcard
- be aware that a risk event form is completed for all reported losses
- never write the password of the Smartcard on the back!

6. Data Quality

Staff who are involved with any data input must comply with the requirement to input accurate and appropriate information and to do so in a timely fashion. It is not just "admin that can wait" If you delay, the appropriate information may not be available to your colleague and patient care can be affected. For example you may not think that Casenote Tracking is very important but failure to log that records have been moved from an office in one building to an office elsewhere can result in records not being available for Outpatient Appointments or urgent admissions with the possibility of very serious clinical consequences for the patient, simply because they cant be found to be provided. The basic rules are:

- staff must take care when entering data and always check the information with an appropriate source
- staff must ensure that they have received adequate training on the system or procedure that they are using
- staff must ensure that they have the relevant procedures to accessible to them at all times
- staff must report errors or omissions that they identify during the course of their work
- staff must be aware that changes will be introduced to ensure that the NHS number is used as the key identifier in line with the Safer Practice Notice

Specific to manual medical records:

- all medical records must have their casenote tracking details changed on every movement (with the exception of records that are supplied by the Library directly to clinics or wards)

- all inpatient episodic information must be collated and filed in a plastic wallet which is secured in to the main medical record before any medical record leaves the ward for any purpose, including Coding
- the Coding function must have access to the full medical record in order to achieve the most accurate coding outcomes
- staff must be familiar with the filing instructions for medical records which are printed on the inside back cover of all lilac records and file every document accordingly

Specific to staff who are working with data eg Information Services, Coding etc

- Staff must take note of guidance which has been publicised and distributed to easily accessible locations in relation to
    - accuracy checks on service user data
    - validating information in relation derived from the recording of clinical/care activity
    - using external data quality reports for monitoring data

- Staff assigned responsibility for Information Quality and Records Management Assurance must ensure that they have been appropriately trained to carry out their role

7. Use of Patient Information

Patients have significant rights to know how the Trust manages the information we hold about them and also to be consulted when their records are being accessed for reasons unconnected to their direct healthcare. This is called Secondary Uses of Data. Examples would be locally agreed Research or access relating to the commissioning process.

All staff who deal with patients must be ready and willing to talk to patients about how we are using their information and respect the choices that patients make. Staff must

- be aware that if patients want copies of all or part of their medical record, that this is called a Subject Access Request and the process is set out in the 04086 Access to Records Policy and the function carried out by the Access to Records Bureau and that there is a charge for this service. The Bureau also offers a free “viewing only” service but there needs to be at least a weeks notice from the date of the request. The trust application form is on the external website.

- know that patients have no right to have “access to health records folder on demand” whilst an inpatient – this seems in contravention of the first statement of this section but that is not the case – the trust retains responsibility for the safekeeping and integrity of the records and any access that takes place must be chaperoned. Relatives (apart from those with parental responsibilities) have no right to view

- be open and clear about when you are disclosing their information to other staff or to anyone else within or external to this organisation eg patients should be aware and consulted with about intentions to contact Social Services which may be necessary because the patient is transferring to a care home

- check that patients are aware of the choices available regarding the use of their information, for example, a patient may not be aware that if they elect to have a second opinion at another hospital, they can refuse for their records at this hospital to be made available to the new clinician taking on the case. Although in this scenario it would also have to be recorded that you informed them that this might detrimental to their care but as long as they are fully informed they are free to make this decision which must be respected. The only possibility when this might be overridden would be if the patient is being cared for under the arrangements identified in the 11001 Mental Capacity Act Policy

- if you don’t know the answer to the patient query about management of their information, you must find out who can answer detailed questions about the use of patient information – if in any doubt these queries can always be referred to the Information Governance Manager

- be aware that there is a patient information leaflet on the intranet and website called Your Information which you can download or tell patients about

8. Sharing Patient Information

Information sharing between agencies is the key to better and more efficient public services but at the same time patients need to be confident that their personal information is kept safe and secure. There are "7 Golden Rules for Information Sharing" which should be

- Remember the Data Protection Act is not a barrier to sharing information
- Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared and seek their agreement unless it is unsafe or inappropriate to do so
- Seek Advice but do not disclose the name of the patient unless it is necessary
- Share with Consent where appropriate and where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your professional judgement, that lack of consent can be overridden in the public interest
- That information sharing decisions are based on considerations of the safety and wellbeing of the person and others who may be affected by their actions
- The sharing must be **necessary, proportionate, relevant, accurate, timely and secure**
- Keep records of your decision and the reason for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose

Data Sharing Agreements (DSA)

When staff find themselves in the position of being asked to routinely share data with another health related organisation which will involve a number of patients being processed in a similar way, then they need to set up a DSA which identifies: what information will be shared with who, how it will be transferred, how will be stored, who is responsible for it and for long will the agreement stands. These can also be used with universities and drug companies involved in research and clinical trials. The Trust publishes signed off DSAs on the website. There is a very simple self explanatory standard form which is available from the Information Governance Manager who needs to retain copies of all agreements in place.

9. Trust Information Assets

The Trust is required to identify its "information assets" ie all the key documents it holds that it needs to maintain its services. All information assets have to be "owned" and the Information Asset Owners (IAOs) in this trust are senior staff down to the level of General Manager or Head of Service. In addition there are Information Asset Administrators (IAAs) who are the staff who manage the asset on a daily basis and there can be only one IAA per asset irrespective of how many staff use an asset, such as a spreadsheet or database on a shared drive.

If you administer an asset you are required to complete an electronic form which is available from your computer desktop. This process covers manual as well as electronic information and applies equally to current and archived information but there would need to be one form per format. Contact the Information Governance Manager if more information is required. There is also 10123 Information Asset Policy on the intranet with more information

10. Freedom of Information (FOI)

Anyone in the world may ask us for trust information and detailed information about the FOI process can be found in 07014 Freedom of Information Policy. Trust information includes: statistics, policies, information about costs or trust charges. It does not cover patient identifiable information. Sometimes the identities of specific staff are requested. In this trust we only release the names, job titles and contact details of staff who have responsibility for decision making or are accountable for the provision of services and never below Band 6.

There are a number of exemptions to the supply of information that can legally be applied and each case is judged on its merits. Also the trust only has 20 days to respond to the request

If you receive a request in writing for information then the request must be forwarded to foi@meht.nhs.uk or if on paper to FOI Requests, Governance, Broomfield Court Annexe.

If you receive a verbal request that in any way concerns the environment (and that could include requests about chemical spillages or plants in the gardens) , then these requests need to be taken down and contact details recorded and passed on as above as they are covered under very slightly different process, the Environmental Information Regulations.

Pay particular attention to complaint letters. It is not unusual for complainants to include an FOI For example, someone may write in to complain about the cost of car parking in the trust and include in that a request to know how much income the trust has received from car parking over the last 5 years. The section about trust income is an FOI. Requesters usually say they are asking for information under the Act, but it does not have to be quoted to be an FOI request.

It is imperative that staff recognise a request but do not answer it even if they know the answer because a Freedom of Information response is compiled in a particular way and provides other information such as how to appeal if not satisfied with the trust response and if this process is not followed, the enquirer will be disenfranchised from their legal rights however good the response is. Also staff generally will not know about the Public Interest Test and how to apply it or about the legal exemptions and may release information inappropriately.

11. Reporting Incidents

All information governance breaches ie not meeting the requirements of Sections 3 & 4 above are potentially Information Governance Serious Untoward Incidents. A risk event form must be completed on the same day and the Datix code to be used for all and any events is 010 067.

If the event is serious, examples could be: the loss of an unencrypted data stick or laptop with patient information, a patient receiving his own and other patients appointment letters who is going to the BBC or press, or a member of the public on the phone who has found a nursing handover sheet on a bus, **then the matter must be referred immediately to the Trust SIRO, Matt Bushell, and if unavailable, to the Chief Executive.**

12. Training

All new starters to the trust attend induction training and information governance is delivered as part of the Integrated Governance Session. Additionally information governance is included as part of Mandatory Update training. However a basic information governance e-training package is being introduced for all staff with an additional unit of training for those staff with access to patient information. This training must be undertaken annually and when invited, it is a trust requirement that they attend. Attendance will be recorded on the ESR and a completion certificate for each module can be printed for staff to keep in their personal development folders/produce at appraisal sessions.

As a general note, staff should not be undertaking any task that involves the management of patient information if they do not consider themselves adequately trained or competent and must refer this to the line manager who can make arrangements with IT for clinical systems training or contact the Information Governance Manager for other possibilities.

13. Contact Details

Information Governance Manager, Liz Stewart: Liz.Stewart@meht.nhs.uk ext 4536
IT Security Manager, Dave Shrimpton, Infosec@meht.nhs.uk ext 5020
SIRO (Senior Information Risk Owner) Matt Bushell Matt.Bushell@meht.nhs.uk ext 6518
IT Helpdesk ext 5000