NHS
West Essex
Clinical Commissioning Group

Forensic Readiness

Policy Reference: IG07

Brief Summary: This policy sets out the principles the Clinical Commissioning Group (CCG) will embed, throughout the organisation, to ensure that procedures, protocols and processes are in place to react efficiently and effectively to all serious information security related incidents encountered and that subsequently the CCG is forensically ready to act.

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	14/03/2013	Draft	New Document	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.0	03/12/2014	Draft	Amendments made following comments from IG Steering Group	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.1	18/12/2014	Draft	Key Contacts added following amendments	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.2	05/03/2015	Final	Approved by West Essex CCG Board	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.0	07/10/2016	Final	Review approved by West Essex CCG's Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex CCG	**Information Governance Team**
Approved by	**Executive Committee**
Approval Date	**7th October 2016**
Next Review Date	**March 2019**
Responsibility for Review	**CCG's Information Governance Team**
Audience	**All NHS West Essex CCG officers and staff (which includes temporary staff, contractors and seconded staff).**

Contents

1. Introduction

Forensic readiness is a key component in the management of NHS information risk. This policy provides the framework within which NHS West Essex Clinical Commissioning Group describes the Forensic Readiness Policy for computer users and sets out the introduction of IG forensic readiness into the business processes and functions of the CCG. The introduction of this policy should maximise the CCG's potential to use digital evidence whilst minimising the costs of forensic investigation.

This policy reflects the high level of importance placed upon minimising the impacts of information security events and safeguarding the interests of patients, staff and the CCG itself.

The aim of the Forensics Readiness Policy is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required from a formal dispute or legal process. The policy may include evidence in the form of log files, e-mails, back up data, mobile computing, network, removable media and others that may be collected in advance of an event or dispute occurring.

The CCG acknowledges that IG forensics provides a means to help prevent and manage the impact of important business risks. IG evidence can support a legal defence, it can verify and may show that due care was taken in a particular transaction or process and may be important for internal disciplinary actions.

2. Purpose

The purpose of this policy is to ensure that:

- NHS requirements relating to security and confidentiality of equipment and information and the requirements of the Data Protection Act are met
- Protect the CCG, its staff and its patients through the availability of reliable digital evidence gathered from its systems and processes
- Allow consistent, rapid investigation of major events or incidents with minimum disruption to CCG business
- Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required
- Demonstrate due diligence and good governance of the CCG's information assets

Benefits

The benefits to the organisation of creating a Forensic Readiness Policy include the following:

- Enterprise defence mechanisms are captured
- It acts as a deterrent to insider threats
- In the event of an incident, this would enable minimum disruption and also link in to the CCG Business Continuity plans
- Reduced cost and time for internal investigations
- Extends information security to the wider threat from cyber crime
- Demonstrates due diligence and good enterprise governance arrangements
- Compliance with the NHS Information Governance Toolkit and other regulatory requirements
- Improves the prospects for successful legal action if required
- Supports employee sanctions based on digital evidence.

3. Scope

This policy applies to all systems and networks used by CCG staff for**:**

- The transmission of non-clinical data and images
- The transmission of clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of internet systems for receiving, sending and storing non-clinical or clinical data or images

4. Definitions & Terms

IG Forensic Readiness

The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption and / or cost.

IG Forensic Readiness Planning

Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence, related monitoring and collection processes and capabilities, storage requirements and costs.

5. Roles & Responsibilities

5.1 Accountable Officers for NHS West Essex CCG

The Chief Officer (CO), as the Accountable Officer, has overall responsibility for information governance within the CCG. The CO is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The CO has delegated operational responsibility for information governance to the Director of Finance, Contracting and Performance.

5.2 Senior Information Risk Owner (SIRO) for NHS West Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Director of Finance, Contracting and Performance. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Audit Committee. This includes oversight of information security incident reporting and response arrangements.

5.3 Caldicott Guardian for NHS West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service users information and enabling appropriate information sharing. For the CCG, this is an executive, the Chief Medical Officer. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

5.4 All Staff

The majority of staff handle information in one form or another. Staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.

The CCG policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance. All staff are required to assist in the identification of information governance issues / breaches and bring them to the attention of the relevant manager.

5.5 Information Asset Owners (IAOs)

CCG information Asset Owners (IAOs) shall ensure that IG forensic readiness planning is adequately considered and documented for all information assets where they have been assigned 'ownership'. Goals for IG forensic planning include:

- Ability to gather digital evidence without interfering with business processes
- Prioritising digital evidence gathering to those processes that may significantly impact the CCG, its staff and patients;
- Allow investigation to proceed at a cost in proportion to the incident or event;
- Minimise business disruptions to the CCG.
- Ensure digital evidence makes a positive impact on the outcome of any investigation, dispute or legal action.

IAOs shall submit their plans for IG forensic readiness to the SIRO for review along with details of any planning assumptions or external dependencies. Forensic readiness plans shall include specific actions with expected completion dates.

5.6 Information Asset Administrators (IAAs)

Information Asset Owners can appoint Information Asset Administrators (IAAs) to support in the delivery of their information risk management responsibilities. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their Information Asset Owner on incident management and ensure that information asset registers are accurate and up to date.

5.7 Head of Information Governance

Will be responsible for:

- Issuing guidance for implementing and compliance with the Forensic Readiness Policy
- Developing and issuing procedures to be followed if misuse is suspected (See Appendices 1 and 2).
- Monitoring performance through quality control and internal audits
- Identifying where improvements could be made
- Reporting performance standards to the Information Governance Steering Group.

Defining the business scenarios that may require digital evidence including:

a) Employee internet misuse / abuse
b) Employee e-mail misuse / abuse
c) Employee performance issues
d) Electronic bullying / harassment
e) Formal Police / legal request for digital evidence
f) Social networking evidence
g) Fraud
h) CCTV
i) Production of audit logs
j) Back up data
k) Removal media
l) Network intrusion / prevention audit records such as cyber – attacks (hacking attempts and so on)

m) Mobile phone and desk phone investigation

5.8 Directors / Associate Directors

The directors / associate directors will support and enable the heads of departments or services to fulfil their responsibilities and ensure the effective implementation of the Information Governance framework.

5.9 Heads of Department

Heads of departments are responsible for ensuring that their service operates within the Information Governance framework. They will ensure that:

- There are effective methods for communicating Information Governance related issues within their service
- Staff completes relevant training, and mandatory updates in relation to Information Governance
- Staff are aware of and adhere to Information Governance policies
- Necessary risk assessments are undertaken within their area of responsibility.
- Information Governance issues and risks are discussed in team meetings.

6. Incident Reporting (Including Near Miss events)

Incidents or near misses that constitute any actual or potential breach of data confidentiality must be reported directly to the Head of Information Governance immediately. An incident form must be completed and submitted in accordance with the CCG’s incident reporting procedures.

7. Forensic Readiness Planning

In order to plan for a digital investigation this organisation needs to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. The following steps describe the key activities needed for this process:

- Define the business scenarios that require digital evidence
- Identify available sources and different types of potential evidence
- Determine the evidence collection requirement
- Establish a capability for securely gathering legally admissible evidence to meet the requirements
- Establish a policy for secure storage and handling of potential evidence
- Ensure monitoring is targeted to detect and deter major incidents

- Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched
- Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence
- Document an evidence based case describing the incident and its impact
- Ensure legal review to facilitate action in response to the incident.

8. Audit & Monitoring Compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

IG Incidents
Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility for providing assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect the framework. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programmes and progress reports
- Reporting Information Governance Toolkit (IGT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

Any incidents reported using the CCG incident reporting process will be monitored to identify breaches to this policy and such incidents will be investigated.

9. Dissemination & Implementation

The policy will be published on the intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

This document will be subject to review when any of the following occur:

- The adoption of the standards highlights errors and omissions in its content
- Where other standards / guidance issued by the CCG conflict with the information contained
- Where good practice evolves to the extent that revision would bring about improvement
- 2 year elapse after approval of the current version.

10. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

11. Related Documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

- Information Governance Policy
- Acceptable use of E Comms and Devices Policy

- Information & Cyber Security Policy
- Acceptable Use of IT Policy (NEL CSU)

12. Equality and Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

13. Key Contacts within the CCG

Within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net

APPENDIX 1

FORENSIC READINESS PROCEDURE

If you suspect inappropriate usage of computer equipment you should contact your IAO / line manager or, the Information Governance Team.

Consideration should be given to the strength of case required to proceed, therefore a preliminary business impact assessment should be made based on whether any of the following are present:

- Evidence of a reported crime
- Evidence of internal fraud, theft or other loss.
- Estimate of possible damages (a threshold may induce an escalation trigger)
- Potential for embarrassment / reputation loss
- Any immediate impact on customers, partners or profitability
- Recovery plans have been enacted or are required
- The incident is reportable under a compliance regime
- If fraud is suspected, then contact the Local Counter Fraud Specialist immediately

Following consideration of the above, the Information Governance Team may be contacted for advice or to request an investigation.

Where there is a requirement for an investigation to be undertaken you should ensure the following steps are taken:

- If you are able to leave everything as it is until the investigator arrives
- Do not leave equipment unattended
- Make sure it is not accessed by anyone at any time

Where this is not possible the following should be applied.

Computer equipment which is switched on:

- Secure the area containing the equipment
- If the user is present ask them to step away from the computer. Do not allow them to close programmes or shut the machine down
- Move people away from the computer and power supplies and do not allow the user or anyone else to touch the machine in any way
- If the computer is directly connected to other computers or equipment (other than via a recognised network data point) then these other machines will need to be dealt in the same manner as outlined in this procedure
- If the computer is attached to the network remove the network cable from the data point.
- Do not touch the mouse or keyboard
- Do not take advice from the computer owner / users
- Allow any printers to finish printing (further evidence may be printing).

If you have to remove equipment before the investigator arrives, the following steps must be performed:

- Record what is on the screen and take a photograph if possible (Note: for laptops, be aware that some power up automatically when the lid is lifted – therefore do not open the lid to photograph the screen and keyboard until battery and power cable has been removed).
- Do not attempt to `shut down' the machine or use the power button
- Switch off the computer by pulling the power cable from the computer, not from the power socket (Note: for laptops, remove the battery before pulling the power cable. When removing the power supply always remove the end attached to the computer and not the socket. This will avoid data being written to the hard drive if an uninterruptable power device is fitted).
- Search the surrounding area and locate any memory devices (for example CDs, DVDs and USB Memory Sticks) that may be associated with the computer in question. Be aware that such devices can take many forms such as USB memory drives being incorporated into key rings and novelty desk items and so on.
- Label and photograph (if possible) all the components in-situ. If no camera is available draw a sketch plan
- Label the ports and cables so that the computer can be reconstructed at a later date
- Carefully remove the equipment and record serial numbers (each component will have a separate number). Also note the identity and serial numbers of any connected devices (for example printer, external hard disk or other memory devices)
- Ensure all items have signed and completed exhibit labels attached.
- Search the immediate area for diaries, notebooks or pieces of paper that may contain passwords
- Consider asking the user if there are any passwords and if these are given record them accurately
- Make detailed notes of all actions in relation to the seizure of computer equipment
- Remove the equipment to a secure location until the investigator arrives.

Upon discovery of computer equipment which is switched off:

- **Do not switch the computer on**
- Secure and take control of the area controlling the equipment
- Allow any printers to finish printing (further evidence may be printing)
- Move people away from any computers and power supplies.
- Confirm the computer is actually switched off – some screen savers can give the appearance that some computers are switched off but hard drive and monitor lights may indicate this is switched on
- Be aware some laptops may power on by opening the lid
- Remove the battery from laptops

- Unplug the power supply from the computer. A computer that is apparently switched off may be in sleep mode and may be accessed remotely, allowing the alteration or deletion of data.

Removable media

Where removable media, that is, a USB pen, external hard drives and so on is found to have been used inappropriately and / or contains inappropriate content you should contact your line manager, or the Information Governance Team immediately and ensure the device is secured and no longer used until advised otherwise.

APPENDIX 2

Computer Investigation: Possessing, Making and Distributing Indecent Images of Children

Possession of Indecent Photographs / Images of Children

It is important to note that the possession of material depicting indecent images of children is a serious criminal offence. Section 160 of the Criminal Justice Act provides:

It is an offence for a person

- To have any indecent photograph or pseudo photograph of a child in his or her possession

Where a person is charged with an offence under this subsection of the Act, it shall be a defence for them to prove:

- That they had legitimate reason for having the photograph in his possession or;
- That they had not themselves seen the photograph and did know or have cause to suspect it to be indecent or;
- That the photograph was sent to him / her without any prior request made by him / her or on their behalf and that they did not keep it for an unreasonable time.

Making and Distributing indecent Photographs / Images of Children

The Protection of Children Act 1978, section 1 provides:

It is an offence for a person:

- To take a permit to be taken, or to make an indecent photograph or pseudo photograph of a child or;
- To distribute or show such indecent photographs or pseudo photographs or;
- To have in his possession such indecent photographs or pseudo photographs with a view to them being distributed or show by him/herself or other or;
- To publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or pseudo photographs or intends to do so

For the purpose of this Act, a person is to be regarded as distributing an indecent photograph or pseudo photograph if he / she parts with the image, or exposes or offers the image for acquisition by another person.

Where a person is charged with an offence under this subsection it shall be a defence for him/her to prove:

- That he / she had a legitimate reason for distributing or showing the photographs or pseudo photographs or having them in his or her possession.
- That they had not, themselves seen the photograph or pseudo photographs and did not know, nor had any cause to suspect them to be indecent

Definition of a pseudo photograph / image: One that is created by image manipulation software so that the overall appearance of any figure is that of a child. Photographs are defined to include data held on a computer that can be resolved into an image.