NHS
Herts Valleys
Clinical Commissioning Group

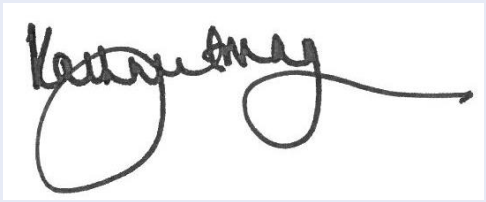
Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		Forensic Readiness Policy
Could this policy be incorporated within an existing policy?	NO	
Does this policy follow the style and format of the agreed template?	YES	
Has the front sheet been completed?	YES	
Is there an appropriate review date?	YES	
Does the contents page reflect the body of the document?	YES	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	YES	
Are all appendices appropriate and/or applicable?	YES	
Have all appropriate stakeholders been consulted?	YES	Information Governance Group
Has an Equality Impact Assessment been undertaken?	YES	
Is there a clear plan for implementation?	YES	
Has the document control sheet been completed?	YES	
Are key references cited and supporting documents referenced?	YES	
Does the document identify which Committee/Group will approve it?	YES	Executive Team

Plans for communicating policy to – staff; practice membership; public (as appropriate)	YES	Via Staff New Bulletin

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Caroline Hall	Date	08.01.18
Signature			

Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Kathryn Magson	Date	08.01.18
Signature			

NHS
Herts Valleys
Clinical Commissioning Group

Forensic Readiness Policy

Version Number	2.0
Ratified By	Executive Team
Date Ratified	January 2018
Name of Originator/Author	Ruth Boughton, Information Governance Manager
Responsible Director	Caroline Hall (SIRO)
Staff Audience	All Staff
Next Review Date	January 2019
Date Issued	

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
v1.0	All	HBL ICT version	March 2014	HBL ICT
v1.1	All	Annual Review and update	July 2015	ENW
V1.2	All	Review and update	August 2015	NS
V2	All	Review and update	November 2017	RB

Contents:

1. INTRODUCTION

Forensic readiness is a key component in the management of NHS Information risk. A directive from David Nicholson stated that all organisations are required to have Forensic Readiness Policies; therefore Information Governance forensic readiness must be introduced into the business processes and functions of the Trust.

This policy provides the framework within which the HVCCG (Herts Valleys CCG) describes the Forensic Readiness Policy for computer users and sets out the introduction of Information Governance (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 directive 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, emails, 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

This policy sets out the context and process for Forensic Readiness in the CCG, thereby ensuring 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

The policy also 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

Benefits

The benefits to the organisation of creating a forensic readiness policy consist of the following:

- Enterprise defence mechanisms are captured
- 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.
- Improve the prospects for successful legal action if required
- Supports employee sanctions based on digital evidence.

3. DEFINITIONS

a. IG Forensic Readiness

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

b. 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.

4. ROLES AND RESPONSIBILITIES

4.1 The Chief Executive

The Chief Executive will maintain ultimate accountability for the implementation of this policy, although specific responsibility will be delegated to others within the CCG.

The CCG will take all reasonable steps to ensure that all staff are aware of policies, protocols, procedures and legal obligations relating to forensic readiness.

4.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of IG forensic policy procedures and standards for the CCG.

The SIRO is responsible for the on-going development and day-to-day management of the IG forensic policy within the CCG's overall Risk Management Programme.

4.3 CCG Information Governance Manager /Head of ICT

Will be responsible for:

- Issuing guidance for implementing and compliance with the Forensic Readiness Policy.
- Monitoring performance through quality control and internal audits
- Identifying where improvements could be made
- Reporting performance standards to the Senior Leaders Team.

Defining the business scenarios that may require digital evidence including:

a) Employee internet misuse / abuse
b) Employee Email 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 etc.
m) Mobile phone and desk phone investigation

4.4 Information Asset Owners (IAO)

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 Trust, its staff and its patients;
- Allow investigation to proceed at a cost in proportion to the incident or event;
- Minimise business disruptions to the Trust.
- 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.

4.5 Directors/Associate Directors

The Directors/Associate Directors will support and enable the Heads of to fulfil their responsibilities and ensure the effective implementation of the Information Governance framework.

4.6 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 complete, 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.

4.7 All Staff

Individual staff members will:

- Be aware of and adhere to relevant information governance policies and procedures
- Complete Information governance training and mandatory updates
- Assist in identification of information governance issues/breaches and bring them to the attention of the relevant manager.

4.8 INCIDENT REPORTING (INCLUDING NEAR MISS)

Incidents (or near misses) that constitute any actual or potential breach of data confidentiality must be reported directly to the CCG Information Governance Manager immediately. An incident form must be completed and submitted in accordance with the CCGs Incident Reporting procedures.

4.9 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.

5. MONITORING COMPLIANCE

5.1 REVIEW AND REVISION ARRANGEMENTS

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

- 1 year has elapsed after approval of the current version

5.2 PROCESS FOR MONITORING COMPLIANCE AND EFFECTIVENESS

The "Information Governance Steering group", will monitor the implementation of this policy, with any supporting procedures, and subsequent revisions.

6. EDUCATION AND TRAINING

Information Governance (IG) Training:

All staff must complete, as part of their corporate induction, a brief introductory training session on information governance. At a later date, (usually within 3 months from start date) all staff will complete approved information governance training, varying dependent on the specifics of assigned job roles. All staff must complete,
annually mandatory information governance training via one of the two approved methods;

1. Classroom style sessions co-ordinated by the IG team
2. Role related, relevant module/s with the E Health Learning Platform

7. REFERENCES

Data Protection Act 1998
Human Rights Act
Freedom of Information Act 2000
Environmental Regulations Act 2005
Access to Health Records Act 1990 (Where not superseded by the Data Protection Act 1998)
Computer Misuse Act 1990
Copyright, designs and patents Act 1988 (as amended by the Copyright Computer Programs Regulations 1992)
Crime and Disorder Act
Electronic Communications act 2000
Regulations of Investigatory Powers Act 2000

8. ASSOCIATED DOCUMENTATION

HVCCG Information Governance Management Framework
HVCCG Information Governance Strategy
HVCCG Information Governance A Guide for all Staff
HVCCG FOI Policy
HVCCG Information Lifecycle Management Policy
HVCCG Mobile Devices Policy
HVCCG DPA & Confidentiality Policy

HVCCG Email and Internet Policy
HVCCG Information Risk Policy
HVCCG Information Security Policy
HVCCG Safe Haven Policy
HVCCG Sharing Policy
Registration Authority Policy
Fair Processing Notice

APPENDIX 1 – Forensic Readiness Procedure

If you suspect inappropriate usage of computer equipment you should contact your IAO/Line Manager, HVCCG IG Lead, HBL ICT Services Team.

Consideration should be given as 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 HVCCG IG Lead, Line Manager, HBL ICT services 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 programs or shut down the machine
- 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 machine 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 batter 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 (e.g. CDs, DVDs, 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 etc.
- 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 (e.g. 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 i.e. USB pen, external hard-drives etc. is found to have been used inappropriately and/or contains inappropriate content you should contact your Line Manager, HVCCG IG Lead, or HBL ICT Support 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.

APPENDIX 3 - Associated Policy Documents

Title
Data Protection and Confidentiality Policy
Information Security Policy
Safe Haven Policy
Information Sharing Policy
Information Lifecycle Management Policy and Strategy
Information Risk Policy

APPENDIX 4 – Glossary

Term	Definition
ACPO	**Association of Chief Police Officers**
CCG	**Clinical Commissioning Group**
CMA	**Computer Misuse Act**
HBL	**HBL ICT Support Service (Herts Valleys, Bedfordshire, Luton)**
IAO	**Information Asset Owner**
ICT	**Information and Communications Technology**
IGFR	**Information Governance Forensic Readiness**
IM & T	**Information Management and Technology**
PDA	**Personal Digital Assistant**
RAG	**Risk Advisory Group**
SIRO	**Senior Information Risk Owner**

Appendix 5

Equality Analysis - Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.

Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	HVCCG Forensic Readiness Policy
What is it that is being proposed?	Policy provides guidance to the CCG staff.
What are the intended outcome(s) of the proposal	That all CCG staff are aware of their responsibilities and are aware of legal requirements the CCG processes.
Explain why you think a full Equality Impact Assessment is not needed	This policy sets of the requirements for forensic readiness..
On what evidence/information have you based your decision?	The policy refers to processes
How will you monitor the impact of policy or service?	Via the IG Toolkit
How will you report your findings?	To the Senior Leaders Team via toolkit action plans and compliance reports

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is not required.	
Assessors Name and Job title Date	Ruth Boughton Information Governance Manager

	29 November 2017