Cambridgeshire and Peterborough
Clinical Commissioning Group (CCG)

IG FORENSIC READINESS POLICY 2017 - 2019

Approval Process

Lead Author:	Information Governance Manager
Reviewed by:	Information Governance, Business Intelligence & IM&T Steering Group
Approved by:	Information Governance, Business Intelligence & IM&T Steering Group
Ratified by:	Clinical Executive Committee (CEC)
Date ratified:	May 2017
Version:	3
Review date:	April 2019 (or earlier if significant change to local or national requirements)
Valid on:	April 2017

Document Control Sheet

Development and Consultation:	Policy developed in consultation with the IG, BI and IM&T Steering Group and endorsed by the Clinical Executive Committee on behalf of the Governing Body.
Dissemination	All staff will be made aware of this policy through the staff bulletin and a direct link to the CCG website.
Implementation	The SIRO is responsible for monitoring the application of the policy by ensuring that:- • The policy is brought to the attention of all employees • Directors as IAOs and Managers are aware of their responsibilities to implement the policy • Staff are informed as appropriate • Appropriate training and guidance is available to staff • Corporate business processes support the implementation of the policy.
Training	Training will be considered as part of the CCG's ongoing processes.
Audit	Implementation of the Policy will be monitored on a regular basis.
Review	This policy will be reviewed two yearly, or earlier if there are changes in procedures or legislation.
Links with other CCG Policies	The Policy should be read in conjunction with: CCG Code of Confidentiality CCG Information Security for Staff Policy CCG Safe Haven Policy CCG Removable Media Policy
Equality and Diversity	The Corporate Services Support Manager (E&D) carried out a Rapid Equality & Diversity Impact assessment and concluded the policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

Revisions

Version	Page/ Para No	Description of change	Date approved
1		Based on an approved example provided by CfH	April 2013
1.1	Links with other Documents	Updated policy list	
2.0		Reviewed and ratified by CMET for 2015-17	July 2015
3	Whole document	Bi-annual review and update	April 2017

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG) Information Governance (IG) Forensics Policy

1. Introduction

The Governing Body has approved the introduction of IG forensic readiness into the business processes and functions of the Trust. This should maximise the potential to use digital evidence whilst minimising the costs of investigation. This decision 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 Governing Body recognises that the aim of IG forensics is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required for formal dispute or legal process. In this context, IG forensics may include evidence in the form of log files, emails, back-up data, removable media, portable computers, and network and telephone records amongst others that may be collected in advance of an event or dispute occurring.

The Governing Body acknowledges that IG forensics provide 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.

This policy is applicable to all areas of the CCG and adherence should be included in all contracts for outsourced or shared services.

2. Definitions

Key definitions are:

- **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 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'.

3. Policy objectives

The IG Forensics Policy has been created to:

- 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 Trust 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;

4. Policy scope

This policy is applicable to all areas of the CCG and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

5. Responsibilities and contacts

SIRO

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

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

The SIRO should be kept informed of significant information governance issues.

The SIRO shall advise the Governing Body on forensic readiness planning and provide exception reports as required.

IAOs

CCG Information Asset Owners (Directors are 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;
- Allowing 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.
- Forensic readiness plans shall include specific actions with expected completion dates.

The Information Governance and IM&T Steering Group

The IG, BI and IM&T Steering Group ensure the development and approval of all IG, BI and IM&T policies and procedures for CEC endorsement on behalf of the Governing Body.

6. Forensic readiness procedure

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. When developing file structures (Information Assets) the following points should be considered:

- Define the type of business scenarios that may require digital evidence

- Establish capability for securely gathering legally admissible evidence to meet the requirement
- Establish 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
- Develop knowledge and awareness in relevant staff members, so that all those likely to be involved understand their role in the digital evidence process and the legal sensitivities of evidence.

Communication
This policy is to be made available to all CCG staff and observed by all members of staff, both clinical and administrative.

Related policies/guidelines
Code of Confidentiality for Staff
Information Security for Staff Policy
Removable Media Policy

Related legal and regulatory requirements
IG Toolkit Requirement – Standard CCG V13-344 includes monitoring requirements.