Forensic Readiness Policy

|REFERENCE NUMBER| 0v1 February 2013|
|VERSION| V1.0|
|APPROVING COMMITTEE & DATE| Clinical Executive Committee 12.2.13|
|REVIEW DUE DATE| February 2016|
West Lancashire CCG is committed to ensuring that, as far as it is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on the basis of their age, disability, gender, race, religion/belief or sexual orientation.

Should a member of staff or any other person require access to this policy in another language or format (such as Braille or large print) they can do so by contacting the West Lancashire CCG who will do its utmost to support and develop equitable access to all policies.

Senior managers within the CCG have a responsibility for ensuring that a system is in place for their area of responsibility that keeps staff up to date with new policy changes.

It is the responsibility of all staff employed directly or indirectly by the CCG to make themselves aware of the policies and procedures of that CCG.
# CONTENTS

## PAGE

1. **PURPOSE**  
   - Purpose: 5
   - Benefits: 5
   - Definitions: 5

2. **SCOPE**  
   - Purpose: 4

3. **GUIDANCE**  
   - Purpose: 4
   - Benefits: 5
   - Definitions: 5

4. **ROLES RESPONSIBILITIES AND ACCOUNTABILITIES**  
   - Chief Officer: 6
   - Senior Information Risk Owner: 6
   - Managers: 6
   - Information Security Manager CSU: 7
   - Head of IT CSU: 7
   - CCG Staff: 7

5. **REFERENCES AND BIBLIOGRAPHY**  
   - 7

6. **ASSOCIATED DOCUMENTS**  
   - 8
1.0 PURPOSE

Forensic readiness is a key component of NHS information risk. In September 2008, a directive from David Nicholson stated that all organisations are required to have Forensic Readiness Polices in place by 2009/2010; therefore information governance forensic readiness must be introduced into the business processes and functions of NHS West Lancashire Clinical Commissioning Group (CCG).

This will maximise NHS West Lancashire CCG potential to use digital evidence whilst minimising the cost of an investigation.

This directive reflects the high level of importance placed upon minimising the impacts of information security incidents and safeguarding the interests of patients, staff and the organisation.

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.

2.0 SCOPE

This policy applies to all staff employed by or working on behalf of NHS West Lancashire CCG including contracted, non-contracted, temporary, honorary, secondments, bank, agency, students, volunteers or locums.

It is the responsibility of all staff (including those on temporary or honorary contracts), agency staff and students to comply with this policy.

Compliance with NHS West Lancashire CCG policies is a condition of employment, and breaching a policy may result in disciplinary action or lead to prosecution under UK law.

It should be noted that the duty of confidentiality is a permanent obligation for an individual, extending beyond the period of NHS employment.

3.0 GUIDANCE

Lancashire Commissioning Support Unit (CSU) IT Team maintains the computer systems and network for NHS West Lancashire CCG. This policy applies to all systems and networks used by NHS West Lancashire CCG staff, for:

- The transmission of non-clinical data and images
- The transmission of clinical data and image
• 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

3.1 Purpose

This policy sets out the context and process for forensic readiness in NHS West Lancashire CCG. The purpose of this policy is to ensure that:

• NHS requirements relating to security and confidentiality of equipment, information and the requirements of the Data Protection Act are met
• Protect the organisation, its staff and its patients through the availability of reliable digital evidence gathered from its systems and processes
• Consistent, rapid investigation of major events or incidents with minimum disruption to NHS West Lancashire 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 organisation’s information assets

3.2 Benefits

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

• IT defence mechanisms are captured
• There is as a deterrent to insider threats
• In the event of an incident, this would enable minimum disruption
• Reduced cost and time for internal investigations
• Extends information security to the wider threat from cyber crime
• Demonstrates due diligence and good information 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

3.3 Definitions

Information governance 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.

Information governance 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, RESPONSIBILITIES AND ACCOUNTABILITIES

4.1 Chief Officer

The Chief Officer will maintain ultimate accountability of the implementation of this policy.

NHS West Lancashire CCG will take all reasonable steps to ensure that staff are aware of policies, protocols, procedures and legal obligations relating to forensic readiness. This will be done through training and staff communications.

4.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of information governance forensic policy procedures and standards for NHS West Lancashire CCG.

The SIRO is responsible for the on-going development and day-to-day management of the information governance Forensic Policy within the organisation’s overall risk management programme.

The SIRO shall advise the Chief Officer and the CCG Governing Body on forensic readiness planning and provide periodic reports and briefings on progress.

4.3 Managers

Managers are responsible for ensuring that their team/area of responsibility operates within the information governance framework. They will ensure that:

- There are effective methods for communicating information governance related issues within their team.
- Staff receive relevant training, induction and mandatory updates in relation to information governance.
- Staff are aware of information governance policies and encourage adherence to them.
- Necessary risk assessments are undertaken within their area of responsibility.
- Information governance issues and risks are discussed at any team meetings.
- Incident reporting is integral to the operational activities within their areas and all incidents are reported and investigated in accordance with NHS West Lancashire CCG policies.
4.4 Information Security Manager Commissioning Support Unit (CSU)

The information security manager at the CSU 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 CCG Clinical Executive Committee.

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 misuse/abuse
g) Fraud
h) CCTV
i) Production of audit logs
j) Back up data
k) Removable media
l) Network intrusion/prevention audit records such as cyber-attacks (hacking attempts etc)
m) CCG issued mobile phone and desk phone investigation

4.5 Head of IT

The CSU Head of IT will be allocated responsibility for assisting the Information Security Manager CSU in the safeguarding of all NHS West Lancashire CCG data and the management arrangements in respect of the organisation’s electronic data processing assets.

4.6 CCG Staff

All staff must be aware of and adhere to relevant information governance policies and procedures

All staff must complete mandatory information governance training yearly and mandatory updates.

5.0 REFERENCES AND BIBLIOGRAPHY

- Good Practice Guide for Computer based Electronic Evidence v.3 Association of Chief Police Officers
- Example Trust IG Forensics Policy www.connectingforhealth.nhs.uk/.../infogov/.../forensicspolicy.doc
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/standards

• NHS Information Security Code of Practice, Connecting for Heath, 2007

6.0 ASSOCIATED DOCUMENTS

<table>
<thead>
<tr>
<th>Document</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email and Internet Policy</td>
<td></td>
</tr>
<tr>
<td>Annual Code of Confidentiality Policy</td>
<td></td>
</tr>
<tr>
<td>Information Governance Training Policy</td>
<td></td>
</tr>
<tr>
<td>Information Security Policy</td>
<td></td>
</tr>
<tr>
<td>Information Governance Policy</td>
<td></td>
</tr>
</tbody>
</table>