The Whittington Hospital NHS
NHS Trust

ITEM: 09/013
Doc: 12

MEETING: Trust Board – 21 January 2009

TITLE: Information Governance Action Plan

SUMMARY:

This paper provides a follow up to the Information Governance (IG) update paper presented to the Trust Board in December 2008.

The paper brings together into a single unified action plan a number of recent NHS Information Governance requirements and audit recommendations resulting from the :-

- NHS Information Governance Assurance Programme (IGAP)
- Serious Untoward Incident (SUI) Action Plan following the "near miss" data loss in September 2008
- Information Governance Independent Review by Cap Gemini on behalf of London SHA

Overall, the Trust is making good progress with implementing the action plan and will continue to be monitored via a monthly Information Governance report to the Executive Committee.

The Trust Board is asked to note the unified Information Governance action plan and the progress made to date.

ACTION: For information

REPORT FROM: Glenn Winteringham, IM&T Consultant

SPONSORED BY: David Sloman, CEO

Financial Validation Lead: Director of Finance	N\A
Compliance with statute, directions, policy, guidance Lead: All directors	NHS Information Governance Assurance Programme (IGAP) ; NHS Information Governance Toolkit ; NHS Confidentiality Code of Conduct ; Data Protection Act

Compliance with Healthcare Commission Core/Developmental Standards Lead: Director of Nursing & Clinical Development	**Reference:** C09, C13a, C13b

Compliance with Auditors' Local Evaluation standards (ALE) Lead: Director of Finance	**Reference:** 5.3

Compliance with requirements of FT application and monitoring regime Lead Director of Strategy & Performance	**Reference:** N\A

1. Introduction

The purpose of this paper is to bring together into a single unified action plan a number of recent Information Governance requirements and audit recommendations resulting from the :-

- **NHS Information Governance Assurance Programme (IGAP)**

  This was initiated by David Nicholson, NHS CEO, in December 2007, following a number of high profile data loss incidents in the public sector *e.g. HM Revenue and Customs loss of 25 million records*

- **Serious Untoward Incident (SUI) Action Plan**

  This was following the "near miss" data loss SUI in July\August 2008

- **Information Governance Independent Review**

  This was undertaken by Cap Gemini in November 2008 and commissioned by London SHA

2. Information Governance Action Plan

Information Governance Requirement	Information Governance Action	Deadline	Status
Information Governance Assurance Programme (IGAP)	Review of security to safeguard bulk transfers of person identifiable data. Ensure that all staff are aware of the risks associated with portable media.	21/12/07	**Achieved**
	Identify other high risk areas and implement appropriate security for any suspended bulk transfers. Complete immediate actions identified in NHS CEO letter of 4/12/07.	31/01/08	**Achieved**
	All Trusts to complete detailed mapping and risk assessment for all data holding systems and data flows. Mitigation for high risk areas established.	29/02/08	**Achieved**
	All Trusts to ensure that all data holding systems and data flows are secure.	31/03/08	**Achieved**
	All Trusts to report Serious Untoward Incidents involving data loss or confidentiality breach in their annual reports.	30/05/08	**Achieved No loss or breach in 07/08**

Information Governance Assurance Programme (IGAP) Cont'd	All Trusts to identify and manage information risks in their annual Statement of Internal Controls.	30/05/08	**Achieved**
	All Trusts to identify a Senior Information Risk Owner (SIRO) at Board level.	30/05/08	**Achieved (David Sloman)**
	All Trusts to encrypt Person Identifiable Data (PID).		
	- Appoint NHS approved encryption specialist supplier	30/12/08	**Achieved**
	- Establish test environment	30/12/08	**Achieved**
	- Encrypt laptops	15/01/09	**Achieved**
	- Encrypt removable media	28/02/09	**In progress**
	- Risk assess PCs and encrypt vulnerable PCs	31/03/09	**In progress**
Serious Untoward Incident (SUI) Action Plan	Where such data exists within applications, the server should be located in a secure environment and access controlled following the Supplier and best practice guides. Where downloads or extracts of data are held, these are to be securely stored on servers with daily back-up and controlled access. If held on networked PCs, then on an encrypted hard disc, again with daily back-up and controlled access	N\A as standard operating procedure	**Achieved**
	Any such databases burned or copied to a portable medium should be stored in a locked cabinet or safe with controlled access. When copies are created, a record should be transmitted to a central register maintained within the IM&T department indicating the date of creation of copies, their location within the Trust and the data items contained therein. This information should be accessible only by designated staff within IM&T, the risk management office and the trust corporate secretary.	28/02/09	**In progress**

Serious Untoward Incident (SUI) Action Plan Cont'd.	All such data held on portable media should be encrypted and password protected	28/02/09	**In progress**
	The transfer of any such portable data within the Trust should be from person to person. No such data should be put in the internal post or left for collection in an unoccupied office.	30/01/09	**In progress** **Revised Information Security Policy approved**
	The transmission of such databases outside the trust should be either via secure electronic transfer as sanctioned by a designated member of the of the IT department or a trust approved courier service	30/01/09	**In progress** **Revised Information Security Policy approved**
	The member of staff initiating the transmission must take responsibility for verifying safe delivery.	30/01/09	**In progress** **Revised Information Security Policy approved**
	The Trust's Confidentiality Policy (January 2008) should be amended to provide specific definitions of the safe storage and transport of confidential data.	30/01/09	**In progress** **Revised Information Security Policy approved**
	The circumstance in which recorded delivery by post is appropriate or recommended should be set out in the Confidentiality Policy and any other relevant procedure documents. The required safeguards to be in place when using recorded delivery should be made clear.	30/01/09	**In progress** **Revised Information Security Policy approved**
	The relevant member of staff should immediately inform the next inline if there is any uncertainty about the arrival of data at its intended destination. If arrival cannot be confirmed, the situation should be escalated up to director level without delay, including details of the data content and the events sequence.	30/01/09	**In progress** **Revised Information Security Policy approved**

Serious Untoward Incident (SUI) Action Plan Cont'd.	Where the manager or director judges that the identification of a risk of missing data is material, statements from all those involved should be sought immediately.		
	If there is any question that the non-location of data could become an SUI, the responsible director must alert the risk management office and the CEO and keep them informed. Any external third parties with a material interest should be alerted and kept informed. Where a loss of data is sufficiently serious to be defined as an SUI, its should be declared as soon as there are reasonable grounds to conclude that the loss has occurred, taking account of the need to avoid unnecessary anxiety on the part of individuals or unnecessary damage to the reputation of the trust.	30/01/09	**Achieved** **Revised SUI Policy approved**
	Searches for missing portable data which form part of a set of multiple copies should firstly establish the location of known copies as a baseline. Forensic examination of existing media should be undertaken immediately to establish as far as possible the timing of creation or copying.	30/01/09	**In progress** **Revised Information Security Policy approved**
	Contingency plans for response to serious incidences of missing confidential data should be drawn up, including communications and helpline protocols, to minimise delay in activation. These plans should include specific arrangements for instances involving data losses which affect third parties.	28/02/09	**In progress**
	The content of induction and refresher training on confidential data should be reviewed and updated.	30/01/09	**In progress Revised Information Security Policy approved**

Serious Untoward Incident (SUI) Action Plan Cont'd.	Managers undertaking staff appraisal should ensure that policies and procedures relating to confidentiality are accessible and fully understood by staff and ensure that PDPs cover any gaps in awareness or understanding.		**Achieved**
	Temporary staff must be closely supervised in any access to or handling of confidential information.	30/01/09	**In progress** **Revised Information Security Policy approved**
	Executive Directors need to ensure that they are familiar with the SUI policy, including escalation processes, and that all managers have appropriate training.	30/01/09	**In progress**
	The importance of following the principles of Prince 2 project management must be reinforced throughout the management structure via the appraisal and development system.	31/03/09	**In progress**
	Technical advice and involvement of the IT department and internal audit must be secured at all stages of the project.	N\A	**Achieved** **Mandated in Trust IM&T Strategy 2008-13**
	The procurement or development of any new database must be submitted for approval through the normal business planning process	N\A	**Achieved** **Mandated in Trust SFIs**
Information Governance Independent Review (Cap Gemini)	Trusts should review existing contracts to ensure that the needs of IGT Requirement 110 are fully met. As a minimum all contracts should contain a description of FOIA and DPA obligations for all parties, how to respond to incidents and information requests from third parties, and clear points of contact.	28/02/09	**In progress**
	Where providing a service to other Trusts, a trust should review (in line with IGT Requirement 110) its legal relationships with its client trusts to ensure that any SLA or other arrangements adequately address IG and IS requirements.	31/03/09	**In progress**

Information Governance Independent Review (Cap Gemini) Cont'd	Trusts should review its relationship with other trusts where a service is shared to ensure that IG and IS obligations are well defined (and legally enforceable), they have been adequately transcribed into policy and procedure, and they are being followed in practice.	31/03/09	**In progress**
	Trusts should ensure that IG and IS responsibilities are clearly defined and understood, particularly if they are split across shared services.	31/03/09	**In progress**
	Trusts should ensure that its managers are adequately aware of the importance of proper project management and the dangers of ad hoc projects.	31/03/09	**In progress**
	Trusts should ensure that staff can seek advice on project management matters similarly to how they can seek advice on IG from the IG manager.	31/03/09	**In progress**
	Trusts should ensure that asset management procedures reflect the demands of IGT Requirement 307, and are integrated into the project management process.	31/03/09	**In progress**
	Trusts should ensure that all physical media are treated as information assets and subjected to asset management processes.	31/03/09	**In progress**
	Trusts should evaluate their current incident reporting system to ensure that reporting thresholds are clearly defined. In case of any doubt, users should be directed to seek immediate advice from the appropriately skilled practitioner e.g. Caldicott guardian, IG/IS officer. Users should also be directed to err on the side of safety and to never delay the reporting process while searches or other evidence are sought.	28/02/09	**In progress** **Incident Reporting Policy to be reviewed**
	Trusts should carefully compare their existing arrangements with those demanded by IGT Requirement 302, particularly those aspects relating to training and awareness of staff with regard	31/03/09	**In progress**

Information Governance Independent Review (Cap Gemini) Cont'd	to incident reporting and the need to inform the IG/IS officers when incidents occur. All staff (including contractors, students, volunteers etc.) should receive incident reporting training that covers all incidents affecting Personal Data during the induction process.		
	Trusts should check that its arrangements for third parties to raise incidents are adequate, that third parties can easily access the information they need to do so, and that they are made aware of the information (as demanded by IGT Requirement 302).	31/03/09	**In progress**
	Trusts should establish clear procedures and guidelines which describe how to gather and log evidence during incident response and SUI investigations. Evidence should be collected into tamper evident containers which are labelled with time and date collected, collector, and collection location, as well as incident ID. Photographs should also be taken where possible.	28/02/09	**In progress** **Incident Reporting and SUI Policies to be reviewed**
	The procedures should describe special measures for use where the object in question cannot be processed as described above, e.g. for large equipment or items in operational use. Contacts for specialist advice should be established in advance for these situations.	28/02/09	**In progress** **Incident Reporting and SUI Policies to be reviewed**
	Trusts should establish clear procedures to be used where child pornography (and potentially other types of extreme material) may be present that clearly forbid the copying of such data even for evidential purposes. A contact should be established with the Police who can advise in such circumstances, and appropriate procedures for Police escalation in these cases defined.	31/03/09	**In progress**

Information Governance Independent Review (Cap Gemini) Cont'd	Trusts should create a search strategy and associated procedures to ensure that searches are efficient and expand as necessary in order to find the missing material. Starting sites should include all locations the missing material has been known to be at any point.	31/03/09	**In progress**
	Trusts should ensure that their SUI policy presents information in the order in which it will be needed. The early stages should be clearly identified and roles and responsibilities as well as reporting and escalation routes, clearly defined. Consideration should be given to presenting information in graphical form so that readers do not miss potential actions, and key decision points are clear. Trusts should ensure that its SUI policy clearly defines SUI to include IG and IS events, such as personal data losses and other disruptive IS events such as computer virus attacks.	28/02/09	**In progress** **SUI Policy to be reviewed**
	Trusts should ensure that its SUI Policy clearly states who are the ex officio and ad hoc members of the investigation panel and how they are to be selected. The selection of the chair should be clearly identified.	28/02/09	**In progress** **SUI Policy to be reviewed**
	Trusts should ensure that the SUI policy considers situations where conflicts of interest might occur. Rules for alternative selection (e.g. as in this case where the CEO asked the Trust Chair to chair the panel) should be defined.	28/02/09	**In progress** **SUI Policy to be reviewed**
	Trusts should consider adding an independent IG or IS professional to SUI panels where IG or IS incidents are being investigated.	N\A	**Achieved**
	Trusts should add the Information Commissioner's Office to the list of external bodies in the SUI policy.	28/02/09	**In progress** **SUI Policy to be reviewed**

Information Governance Independent Review (Cap Gemini) Cont'd	Trusts should involve IG, IS and Data Protection officers, as well as the Caldicott Guardian within the SUI process.	N\A	**Achieved**
	Trusts should ensure that all contracts, where it is acting as a supplier, adequately define expectations and procedures for incident reporting.	31/03/09	**In progress**
	Trusts should ensure that their incident and SUI policies and procedures clearly describe how and when affected third parties, particularly client trusts in shared service arrangements, are informed about incidents.	28/02/09	**In progress** **Incident Reporting and SUI Policies to be reviewed**
	Trusts should define a clear policy which details minimum standards for passwords. This should indicate minimum lengths for passwords used in different situations, and the importance of using passwords which cannot easily be guessed. The policy should ensure that password strength is consistent with the time that the data must be protected by the password, considering that much health data is valuable to an attacker for an extended period.		**Achieved** **Revised Information Security Policy approved**
	Trusts should ensure that all third parties generating their own passwords to protect trust data follow, as a minimum, the trust policy.	31/03/09	**In progress**
	Trusts should consider password generation and vault technologies as part of an overall review of password generation and storage provision.	31/03/09	**In progress**
	Trusts should define a clear policy which details how passwords are to be exchanged with third parties.	N\A	**Achieved** **Revised Information Security Policy approved**

Information Governance Independent Review (Cap Gemini) Cont'd	Trusts should ensure that when exchanging passwords a secure email system (if email is used to exchange) is used and not normal insecure email.	N\A	**Achieved** **Revised Information Security Policy approved**
	Trusts should ensure that asset management policies and procedures are applied to passwords.	31/03/09	**In progress**
	Trusts should audit storage arrangements in each office location to ensure that staff have readily available access to appropriately secure storage containers for sensitive data. The trust should consider fire and waterproof containers where appropriate.	31/03/09	**In progress**
	Trusts should establish strong procedures for the physical storage and handling of sensitive data (in any form).	31/03/09	**In progress**
	Trusts should require that sensitive data is stored in a tamper evident manner -particularly if people without a need to access the data have access to the storage container.	31/03/09	**In progress**
	Trusts should audit disposal arrangements for sensitive data with a view to ensuring robust disposal. All types of media should be considered including: paper, CD/DVD, hard drives and memory sticks.	31/03/09	**In progress**
	Each office area should have well publicised and convenient access to appropriate disposal methods.	31/03/09	**In progress**
	Destruction of any registered assets (e.g. CDs) should be appropriately controlled and logged.	31/03/09	**In progress**
	Trusts should audit physical access controls for all areas handling personal data. The audit should consider the strength of the access controls in use and whether their effectiveness is undermined by poor practice or implementation, as well as	31/03/09	**In progress**

Information Governance Independent Review (Cap Gemini) Cont'd	whether sufficient deterrence exists to discourage criminal activity.		
	Trusts should audit physical access measures for laptops and workstations. All devices should be physically tethered when not stored in secure locations to deter opportunistic theft. Laptop users should be supplied with sufficient tethers so that the devices can be secured at all locations the user operates them in.	31/03/09	**In progress**
	Inactivity screen locks should be enforced for all non-clinical systems. Inactivity lockouts should be considered for clinical workstations, if appropriate. Users should be encouraged to lock their systems when not in use, either via CTRL-ALT-DEL or WIN-L	28/02/09	**In progress** **Revised Information Security Policy approved**
	Trusts should clearly define the procedures for staff to burn CD/DVD. These procedures should require business justification, explanation of purpose for the CD/DVD to be burnt, permission to copy copyright/personal data material (from the owner), as well as any information needed for the container (e.g. handling instructions, contact details), and any asset numbers of source media.	28/02/09	**In progress** **Revised Information Security Policy approved**
	Trusts should ensure that all CD/DVD or similar media that are burnt are entered into a properly controlled asset register. The manufacturer serial number should be included in the register. All media should be permanently marked with the asset number both on the media and on its container. Only blank media supplied by the IM&T department should be used, and only media that has a unique serial number from the manufacturer should be purchased.	28/02/09	**In progress** **Revised Information Security Policy approved**

Information Governance Independent Review (Cap Gemini) Cont'd	The trust should ensure that all media has appropriate protective markings applied, including media supplied by external parties (which should also have its own asset number). Markings, handling instructions, contact details if lost/unreadable should be added to the container1 (e.g. on a CD case insert). Staff should not be permitted to copy any media unless it has a protective marking and trust asset number	28/02/09	**In progress** **Revised Information Security Policy approved**