	Information Governance Assurance Programme – Programme Closure Document			
	Programme	IGAP	Document Record ID Key	
	Sub-Prog / Project		IGAP/PCD/0001	
	Prog. Director	Mike Faulkner	Status	Approved
	Owner	Richard Jeavons (SRO)	Version	1.0
	Author	Mike Faulkner	Version Date	12/08/08

Information Governance Assurance Programme Programme Closure Document

Amendment History:

Version	Date	Amendment History
0.1	27/05/08	First draft for comment
0.2	05/06/08	Second draft incorporating some input from the programme team. Issued to the Programme Board for structure review.
0.3	12/06/08	Third draft incorporating further review comments, feedback from programme board and additional content
0.4	17/06/08	Incorporating additional content from IGAP Programme Exec members. For review at IGAP meeting on 20/06/08
0.5	24/06/08	Incorporating amendments from review meeting on 20/06/08. Issued to IGAP Programme Exec for review meeting on 25/06/08
0.6	26/06/08	Incorporating amendments from review meeting on 25/06/08 and re-draft of section 8 from Phil Walker. Issued to IGAP Programme Board and IGAP Programme Executive for review
0.7	05/07/08	Incorporating comments from review and inclusion of SUI analysis.
0.8	09/07/08	Incorporating amendments from programme executive review on 07/07/08.
0.9	11/07/08	Final draft for approval by the IGAP Programme Board
0.10	14/07/08	Final draft for approval by the IGAP Programme Board, now including reconciled data in the charts in section 5 and appendix 1.
0.11	01/08/08	Amendment to reflect discussions at the IGAP Programme Board review meeting on 21/07/08. Issued to the Programme Board for final approval
1.0	12/08/08	Approved by the Programme Board

Reviewers:

This document must be reviewed by the following

Name	Signature	Title / Responsibility	Date	Version
Richard Jeavons		Director of IT Service Implementation, NHS CFH / DH	12/08/08	1.0
Bob Armstrong		DH Director of Information Services	12/08/08	1.0
Gordon Hextall		Chief Operating Officer, NHS CFH	12/08/08	1.0
Professor Sir Bruce Keogh		NHS Medical Director, and Caldicott Guardian	12/08/08	1.0
Martin Judkins		CIO, West Midlands SHA	12/08/08	1.0
Mike Walker		Director of Digital Information & Health Policy	12/08/08	1.0
Rachel Gregson		Yorkshire & Humber SHA	12/08/08	1.0
Remi Ogbe		IG Manager, Barts and the London NHS Trust	12/08/08	1.0
Gordon Wanless		IG Manager, NHS Business Services Authority	12/08/08	1.0
Peter Jenkinson		Head of Information Services, Ashton Leigh & Wigan PCT	12/08/08	1.0

Alan McDermott		IT Director, NHS Blood & Transplant Authority	12/08/08	1.0
Jeanne Roberts		Royal Collage of Midwives	12/08/08	1.0
Nicola Dunn		Swindon PCT	12/08/08	1.0

Approvals:

This document must be approved by the following:

Name	Signature	Title / Responsibility	Date	Version
Richard Jeavons		SRO and chair of the Information Governance Assurance Programme Board	12/08/08	1.0

Distribution:

To be distributed as per review and approval lists above, the IGAP Programme Executive and IGAP Programme Board Observers.

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in the programme's document repository is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number	Title	Version
1	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated.doc	
2	IGAP-PID-0001	Information Governance Assurance Programme – Programme Initiation Document	V2.0

Glossary of Terms:

Term	Acronym	Definition
Information Governance Assurance Programme	IGAP	The programme to address Information Governance issues and establish an IG Assurance Framework across the DH, NHS, all subsidiary organisations and Arms Length Bodies
Person Identifiable Information	PII	One or more pieces of information that relate to an individual, who can be identified from those pieces of information or identified by combining those pieces of information with other information that is likely to be available. The individuals concerned may be patients, staff, contractors or members of the public.
Sensitive Person Identifiable Information	SPII	Either: <ul style="list-style-type: none"> a) Person Identifiable Information where unauthorised or inappropriate disclosure could cause harm or distress to the individual who is the subject of the information; OR b) A set or grouping of Person Identifiable Information relating to 50 or more individuals regardless of the risk of damage or distress.

Contents

1	Executive Summary	6
2	Introduction.....	8
2.1	Background.....	8
2.2	Purpose.....	8
2.3	Scope.....	8
3	Programme Review.....	9
3.1	Review & Assurance of Existing IG Standards.....	9
3.2	Development & Implementation of an Information Governance Assurance Framework.....	15
3.3	Integration with Governmental and wider reviews.....	19
4	Achievement of Programme Objectives	21
4.1	Objective 1 – Assurance by 31/03/08.....	21
4.2	Objective 2 – Ongoing Assurance	22
4.3	Objective 3 – Robust IG Policies and Procedures.....	23
4.4	Objective 4 – Implement Cabinet Office Minimum Standards	23
5	Benefit Realisation	25
5.1	Increase in organisations using the IGT	25
5.2	Number & Severity of IG SUIs.....	25
5.3	Percentage split on scores for the 16 standards	26
6	Handover and Transition Activities	27
6.1	Incomplete Activities.....	27
6.2	Risks and Issues	32
6.3	Transition Activities	32
7	Programme Documentation.....	33
8	IG Assurance Framework and ongoing organisational structures	35
8.1	IG Assurance Framework.....	35
8.2	DH Organisational Requirements.....	37
8.3	NHS and ALB Organisational Requirements.....	40
	Appendix 1 – Analysis of Sensitive Person Identifiable Information SUIs.....	41
	Appendix 2 – IG Standard (draft).....	45
	Appendix 3 – Programme Milestone Chart.....	48
	Appendix 4 – Risk and Issues Log	51
	Appendix 5 – Summary of Recommendations.....	55

1 Executive Summary

The Information Governance Assurance Programme was initiated in February 2008, in response to the Cabinet Office Data Handling Review (DHR). Its remit was firstly to provide assurances regarding the current processing of person identifiable information, in line with the requirements of the DHR, secondly to produce an Information Governance Assurance Framework for the healthcare sector and thirdly to provide continuing assurance that sensitive person identifiable information is managed securely and confidentially.

Many parts of the DH, its Arms Length Bodies and the NHS were already considerably engaged with the Information Governance agenda, and the NHS Chief Executive had already written to the NHS requiring urgent attention to be paid to key requirements relating to data security. This provided a solid foundation for the programme to build upon.

In undertaking its work, the programme has developed a number of principles, which will support Information Governance work going forwards.

Principles:

- All NHS organisations, NHS provider organisations, the broader "family" of NHS organisations and the DH and its ALBs should as much as possible, be part of the same IG Assurance Framework;
- The IG Assurance Framework is the mechanism by which:
 - IG policies and standards are set;
 - Regulators can check an organisation's compliance;
 - An organisation can be performance managed.
- Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as important as financial and clinical governance in organisational culture;
- The framework will provide assurance to the several audiences interested in the safe custody and use of Sensitive Person Identifiable Information in healthcare. This involves greater transparency in organisational business processes around Information Governance;
- The requirements of the Cabinet Office Data Handling review will be implemented in DH and its ALBs and should, as much as possible, be applied to all NHS organisations.

However, a limiting factor across all organisations is capacity and capability in respect of Information Governance.

The programme has broadly achieved its objectives and reached a natural conclusion. It is therefore closing to ensure that Information Governance returns to a 'business as usual' activity and not to rely upon the existence of a transient programme of work. This document makes a number of recommendations that will facilitate the transition to 'business as usual' and ensure that an appropriate focus on Information Governance is maintained.

Programme Outcomes

The outcomes of the Information Governance Assurance Programme can be summarised as:

- The main components of an Information Governance Assurance Framework have been established;
- The existing NHS policy framework has been strengthened, and clarified to reflect the Cabinet Office Data Handling Review. This has been translated into a clear set of IG requirements applicable to all organisations;
- The IG Toolkit has been developed as the principle mechanism by which IG policy can be synthesised into measurable requirements for IG. It demonstrates how organisations can be assessed in terms of performance. Its output will be used to inform not only those concerned with policy, e.g. the NIGB, but also those concerned with assessing performance, including Monitor and SHAs;
- The critical importance of compliance with the IG requirements has been firmly established on the agendas of Boards, Audit Committees, executive and non executive Directors;
- The requirement for internal audit of IG has been formally established by including IG performance in the Statements of Internal control, and the potential established to further enhance assurance via external audit;
- The principle regulatory bodies have included IG assurance on their performance assessment and management agendas; most notably the Healthcare Commission, but also Monitor in respect of Foundation Trusts;
- The management of information risk has been strengthened by new requirements for senior information risk owners, and a clarified role for a supporting framework of information asset owners within each major organisation;
- A substantial start has been made to the task of building capability and capacity by launching important training initiatives, which have been very well received. This has been done by ensuring that IG is included in the advisory and support material available to Board members.

Appendix 5 summarise the recommendations made within this document. Individual owners for each recommendation have been determined and agreed. One of the recommendations is that the newly appointed CIO for Health is the focal point for Information Governance, and is accountable to the Permanent Secretary and the NHS Chief Executive for the delivery and maintenance of the Information Governance Assurance Framework (Recommendation 27). As such, the CIO for Health should be responsible for ensuring that once this document is approved by the Informatics Executive Group (the IGAP sponsoring body) the recommendations are implemented by the owners identified in Appendix 5.

2 Introduction

2.1 Background

The Information Governance Assurance Programme was initiated in February 2008, with formal approval of the Programme Initiation Document (*ref 2*) at the second Programme Board meeting on 12th March 2008.

The Programme was established to provide assurance to the public, key stakeholders and Ministers that Person Identifiable Information (PID) held within, and transferred between, the Department, its ALBs, healthcare providers, delivery partners and support services is managed in a secure and confidential manner. The programme was also tasked with producing an Information Governance Assurance Framework applicable to all parts of the healthcare sector, and to provide continuing assurance that PID is managed securely and confidentially.

2.2 Purpose

The purpose of this document is to review the programme, and to set out all the actions and activities that have taken place that will allow it to close. Once approved by the Programme Board it will be the confirmation that:

- The programme has achieved its objectives¹;
- All projects have completed satisfactorily;
- Any remaining handover or transition activities required have been defined and assigned to relevant business operations.

This document also contains recommendations for the Department of Health, where the programme team and the programme board feel that these are appropriate, in order to ensure that the Department and its constituent organisations can continue to deal effectively with Information Governance issues.

2.3 Scope

This document covers all of the activities within the scope of the Information Governance Assurance Programme, as documented in the Programme Initiation Document (*ref 2*).

The content of this document meets OGC best practice as set out in its publication “Managing Successful Programmes”, covering:

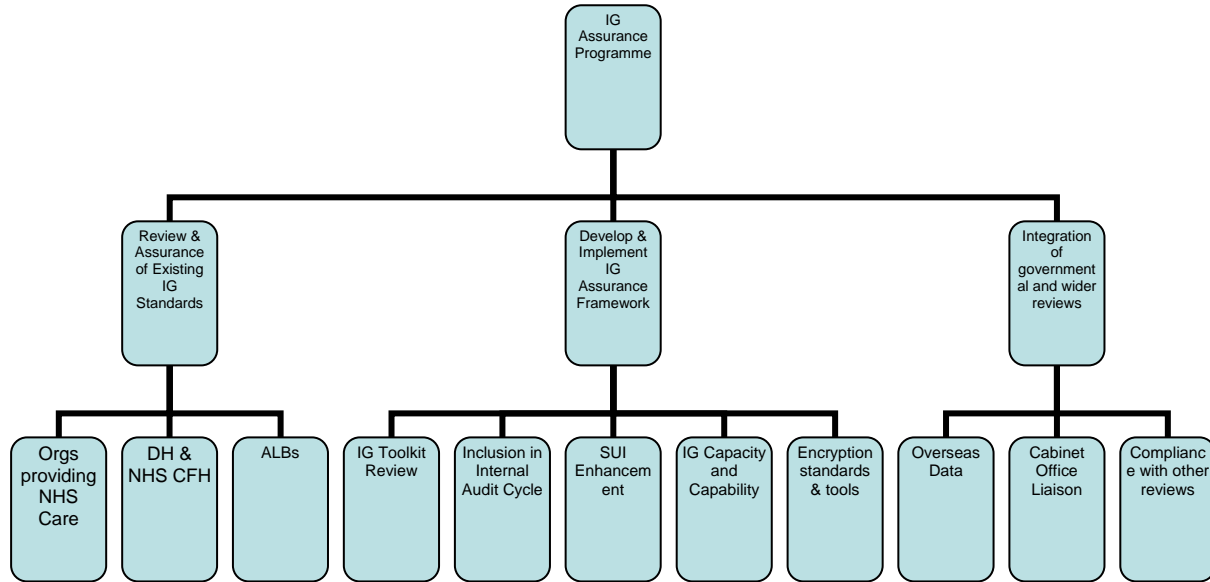
- A review of the programme (sections 4 and 3);
- Update and finalisation of all programme information (section 7);
- Feedback to policy and strategy (sections 4 and 5);
- Confirmation that remaining/ongoing activities can be handled by ‘business as usual’ (sections 6 and 8).

¹ Managing Successful Programmes records this as “The Business Case has been satisfied”. This has been replaced with achievement of objectives, as this programme did not have a business case in the conventional sense due to its nature.

3 Programme Review

As documented in the PID (ref 2), the programme was divided into three workstreams as per Figure 1. The following sections review the achievements of each of these.

Figure 1: WORKSTREAM OVERVIEW



3.1 Review & Assurance of Existing IG Standards

The purpose of this group of activities was to obtain immediate assurance that the processing² of sensitive person identifiable information by in scope organisations is secure and confidential, in accordance with the current Information Governance Toolkit and all relevant guidance. This was broken down into three different areas according to the type of organisation, which are covered in the following sections.

In order to ensure that the programme was addressing all relevant organisations and their systems links were made to a separate project, already initiated by DH, to map the relationship between the department and the non-statutory organisations, which it has established and continues to fund. Out of this continuing piece of work a provisional list of all the different organisations

² “processing”, [as defined by the Data Protection Act] in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

within the “enterprise” has been identified, building upon the list that can be found in Appendix 3 of the PID (*ref 2*). This list also includes the lines of accountability. This list and lines of accountability should be maintained as a valuable (and necessary) resource for the Department of Health in managing its business. However, as a fundamental principle, any organisation in which such a body is hosted must treat the hosted body as part of its own organisation for the purposes of information governance.

Recommendation 1.	<i>Any organisation which hosts another body within it must treat that body as part of its own organisation for the purposes of information governance.</i>
--------------------------	---

Recommendation 2.	<i>The list of organisations and lines of accountability of all such non-statutory bodies should be owned and maintained centrally within the Department of Health as a valuable resource for managing its business.</i>
--------------------------	--

3.1.1 Organisations providing NHS Care

Acute Trusts, PCTs, Mental Health Trusts, Ambulance Trusts and SHAs were provided with a detailed project plan that set out the stages, tasks, responsibilities and expected outcomes of an initial assurance process. Tasks and Outcomes for each of the phases are provided below:

	Expected Outcomes	Tasks	Report Deadline
1	<p>Assurance to be provided by Trust CEO that:</p> <ul style="list-style-type: none"> • All bulk transfers of P.I.D have been identified and reviewed. • Remedial action has been taken to suspend insecure bulk flows of P.I.D. 	<ul style="list-style-type: none"> • Identify, risk-assess and document data flows on spreadsheet provided. 	21/12/07
2	<p>Assurance to be provided by Trusts that:</p> <ul style="list-style-type: none"> • Remedial action has been taken in regard of insecure bulk flows of P.I.D • All bulk transfers of P.I.D are secure • Other high risk areas have been identified • Action is being taken to map and review risks for all other (non-bulk) flows of P.I.D 	<ul style="list-style-type: none"> • Highlight areas of key risk and implement immediate remedial action as necessary • Assign project lead to co-ordinate and support data mapping process for all other flows of P.I.D. • Assign responsibility to, and inform, department heads to identify and risk assess data-flows within their areas. • Assign project lead(s) to co-ordinate work on the IG standards identified at Annex A 	31/01/08

3	<p>Assurance to be provided by Trusts that:</p> <ul style="list-style-type: none"> • All other (non-bulk) flows of P.I.D have been identified and reviewed. • Remedial action has been taken in regard to risk areas. • All non-bulk flows of P.I.D are secure or risks mitigated. • All required security policies are in place. • An incident reporting policy is in place. 	<ul style="list-style-type: none"> • Carry out review of P.I.D flows using spreadsheet or mapping tool and risk criteria provided by NHS CFH. • Highlight areas of key risk and implement immediate remedial action as necessary. • Review incident reporting procedures to ensure these include process for reporting/ investigating P.I.D incidents. • Review other procedures relating to transfer of data including courier services, data encryption, confidential waste, etc. 	29/02/08
4	<p>All required assurance to be provided by Trust CEO.</p>	<ul style="list-style-type: none"> • Complete and submit signed Statement of Compliance to NHS CFH. • Complete and submit Information Governance Toolkit assessment (v5). • Complete and submit the assurance statement provided at Annex D to the SHA. 	31/03/08

As required, all CEOs from the larger NHS organisations provided the responses to SHA CEOs as described above. The position regarding Foundation Trusts is described separately below. The responses from the ten SHAs were collated, analysed and reported to David Nicholson, NHS CEO, in May 2008. A summary of IG toolkit assessment returns for all larger NHS organisations was provided to the NIGB, Healthcare Commission, Monitor and SHA CIOs during April/May 2008.

Monitor & Foundation Trusts

In support of the Information Governance Assurance review, Monitor asked all Foundation Trusts to make a declaration of compliance i.e. that policies, procedures, and governance arrangements are in place to support IG assurance. Monitor have confirmed that all Foundation Trusts have either provided declarations of compliance or a declaration which has a caveat, but is supported by action plans where deficiencies were reported. Moving forward we have provided Monitor with detailed IG performance data for Foundation Trusts and have drawn to their attention any poor performing organisations.

Independent contractors

The responsibility of PCT CEOs in respect of independent contractors, in particular GPs, was flagged by David Nicholson in a letter to all NHS CEOs on 15 January 2008. However, it is clear that a lack of capacity, capability and leverage has limited what PCTs have been able to achieve in the timescale of the programme. To some extent this has been mitigated by action at the centre concerning centrally, contracted providers (see section 4.1).

3.1.2 Department of Health and NHS Connecting for Health

An Initial audit of DH systems with person identifiable information was completed by 28/02/08 and further information provided to the Cabinet office.

The DH commissioned Audit Reports covering:

- Provision of data to the National Audit Office
- Data Protection Policies and Procedures
- A review of the DH's inventory of information assets
- Reviews of four selected systems, the Contact correspondence system, the injury Costs Recovery System, MEDBEN and the Abortion database.

Final reports on these studies have been received, and actions are in hand to implement their recommendations. A Findings Matrix to track progress is being prepared.

Reports on progress were provided to the DH Audit Committee in March and June.

An internal DH IGAP plan has been developed based on the findings of the audit reports and the Cabinet Office recommendations set out in the document "Handling Information Risk".

Progress reported in June included:

- Appointment of a SIRO for DH and NHS Connecting for Health.
- Incident reporting arrangements in place
- Initial audit of key information assets containing protected personal data completed
- Arrangements to secure PROTECT level information confirmed and reinforced, covering data held on the DH network, on laptops and removable media, and on paper.

Actions to be completed in July 2008 include:

- Publication of an Information Risk Policy, an Information Charter and a Forensic Readiness Policy
- Implementation of Privacy Impact Assessments for new systems at the scoping and commissioning stages
- Use of new OGC model contract clauses covering information governance
- Identification of Information Asset Owners for key systems
- Development of a high level culture change plan.

Actions to be completed by October 2008 include:

- Identification of Information Asset Owners for all DH and NHS CFH information assets
- Trusted mechanism for raising concerns about information risks
- The mechanism to log and consider requests for information access.

Some of the IT systems and databases maintained by NHS CFH are maintained on behalf of the NHS, and are therefore not subject to some of the central government requirements. They are managed according to NHS

Information Governance standards and must be regarded as separate and distinct from other DH systems and databases.

3.1.3 Arms Length Bodies

Following the decision to launch the IGAP programme it was determined that the Department of Health's Arm's Length Bodies (ALBs) were to be fully within the scope of the programme, with the exception of the Commission for Patient and Public Involvement in Health which was due to close on 31st March 2008.

The ALB sector included Executive Agencies, Executive Non-Departmental Public Bodies (ENDPBs) and Special Health Authorities (SpHAs). Some work with the NHS and some with Social Care.

A decision was also made that the departments other public bodies (the advisory non-departmental public bodies) would be outside the scope of the programme, as they had no executive functions (having no staff and no budgets).

The outcome for the ALBs was to ensure that each individual organisation would review person identifiable information flows and provide assurance that such information flows are secure and confidential within, to and from the ALB.

Deliverables achieved:

- Internal Audit review of the person identifiable information in the ALBs was carried out during January 2008, along with a judgement of the degree of risk (March 2008);
- Full participation of the ALB sector in the IGAP programme to ensure that common standards apply across the department, its ALBs and the NHS (from February 2008);
- Full participation of the ALB sector in the implementation of the Cabinet Office recommendations, with the objective of achieving the Cabinet Office's target dates:
 - Distribution of the Cabinet Office recommendations to ALBs ((March 2008);
 - Workshop for ALBs to assist with implementing the recommendations (April 2008);
 - Distribution of IGAP update notes (from April 2008 onwards);
 - Distribution of Cabinet Office guidance (from April 2008 onwards);
 - Follow up workshop for ALBs (June 2008);
 - Briefing for ALB Chief Executives and Chairs at a network meeting (July 2008).
- Implementation of assurance processes:
 - ALB Chairs notified of Cabinet Office recommendations and made aware of the role on Boards and/or Audit and Risk Committees in monitoring progress within their organisation;

- ALB data security covered in statements of assurance of DH Directors General who sponsor ALBs (May 2008);
- Reports on progress in implementation of the recommendations made by ALBs to their Senior Departmental Sponsors (SDSs), with the reports tabled and discussed at the 2007-08 quarter four accountability reviews (May and June 2008);
- Analysis of ALB progress based on the above reports to be made by ALB Business Support Unit (June 2008);
- A further report on progress from the ALBs will be required for the 2008-09 quarter two accountability reviews (October and November 2008) and the quarter four accountability reviews (May and June 2009).

3.2 Development & Implementation of an Information Governance Assurance Framework

At the start of the programme there were a number of existing components and activities, all aimed at improving the organisations ability to define, manage and meet Information Governance standards and requirements. These activities all came within the scope of the programme and were described in the PID (*ref 2*). The subsequent sections follow those definitions in the PID and describe what has taken place. However, while all of these components and activities could, in combination, be called an Information Governance Assurance Framework, there is in fact nothing that ties them together into a coherent whole. The work to address this is covered in section 8.1, while this section concentrates on what has been done in relation to those individual items described in the PID.

During the course of the programme there were also a large number of requirements emanating from Cabinet Office, which required further activities within this part of the programme. These are covered in section 4.4

3.2.1 IG Toolkit Review

The components of the Information Governance Toolkit were reviewed by a wide range of bodies and groups, each looking at the aspects that relate most directly to their work areas. A gap analysis was conducted against the requirements of the Cabinet Office Data Handling Review, and a number of minor changes made. Version 6 was then agreed with NIGB at its April meeting. New views of the IGT have been developed to accommodate new organisation types, though these will need refining over the coming year.

It was not possible to update the version of the IGT used by General Practice, as this would have impacted on the contractual delivery of the IM&T DES. Discussions are planned with the GPC and RCGP in July with the aim of bringing the GP view of the IGT back into alignment with the other views in the v7 release.

Work has also begun on the development of a standard for information governance that will underpin the IGT and its further development. Consideration is also being given to mandating minimum standards from March 2009 onwards (see section 8.1.3).

3.2.2 Inclusion of Information Governance in the internal audit cycle and Statement of Internal Controls

In order to ensure that the Information Governance Assurance framework is mainstreamed into the activity of NHS organisations and is considered as a Board level issue, work was undertaken to ensure that the requirements laid down by the NHS Chief Executive of all NHS organisations were reflected in the NHS Finance Manual and supporting guidance. This included explicit reference to IG within Statements of Internal Control and Annual Reports.

The Finance Manual and its supporting guidance for 2009/10 will be issued and consulted upon later in the year. There is agreement that the material will explicitly reflect these requirements. The impact of this is that IG

assurance will be formally considered as part of the risk management regime of each organisation, and formally audited (internally) annually. This includes review by the audit committee; consideration of the outcome by the board; and ultimately the sign off by the Chief Executive and inclusion in the annual report. This will also include specific referencing of IG Serious Untoward Incidents (see below)

In respect of Foundation Trusts, Monitor have provided assurances that they will mirror this activity in respect of the FREM, the Finance Manual equivalent. Therefore, the same regime will apply to Foundation Trusts.

To complete this part of the programme there is ongoing work to include these same provisions, in the form of outputs within the NHS Standard contract, which will have the effect of giving Commissioners the ability to hold provider organisations to account in respect of Information Governance issues, and provide a range of sanctions as appropriate. This will also mean that the same provisions are part of contracts with Independent Sector organisations (see section 6.1.12).

Similar standards and procedures (annual Statements of Internal Control that make specific reference to Information Governance, formally audited by the external auditors, reviewed by the Audit and Risk Committees and signed by the Chief Executive) have been established in DH and its ALBs. In addition, the ALBs' Statements of Internal Control are part of the evidence chain on which the DH Directors-General who sponsors them refers to in their annual Statements of Assurance, on which the DH Statement of Internal Control is based.

External Audit

The Audit Commission, as external auditors of NHS organisation, has indicated in response to consultation its view that the increased emphasis on IG and its inclusion in statements of Internal Control etc. means that it is more pertinent than ever that the role of the auditor is highlighted. There is considerable potential to provide the independent assurance which the DH can expect in relation to these changes.

The Audit Commission has provided a copy of the NHS Chief Executive's letter to all auditors on 27th May with some accompanying guidance notes. Its expectation is that auditors will consider whether the additional reporting requirements have been met. However, this will not involve an in-depth external audit of IG risk management, or the non-financial information reported or the accuracy of statements made in the report.

The Commission has indicated a willingness to discuss further what more work can be undertaken to provide enhanced levels of assurance to the DH. Timescales have not allowed these discussions to be completed, and if required there is an ongoing piece of work to bring this to fruition.

The National Audit Office (NAO), as external auditors of DH and its ALBs, have been fully involved in the increased emphasis on IG in the review of Statements of Internal Control for the department and its ALBs.

Recommendation 3.	<i>Complete discussions with the Audit Commission regarding further NHS Audit activity, including any resource implications.</i>
--------------------------	--

3.2.3 Serious Untoward Incident (SUI) Reporting related to failures in Information Governance

The existing SUI process in respect of data loss and confidentiality breaches was ill defined and not used in a consistent manner. Guidance has been issued to provide a standard way of categorising incidents and ensure that all relevant incidents are reported to the appropriate bodies.

Details of reported SUIs are now published each quarter on SHA websites, and all Trusts are required to include a summary of incidents and the action taken to prevent reoccurrence in their annual reports.

Guidance has also been issued to provide a standard way of categorising incidents for the ALB sector. SUIs arising from ALBs are reported to the ALB Business Support Unit, the ALB's departmental sponsor team and escalated if appropriate to Ministers.

In accordance with Cabinet Office guidance, a summary of incidents and the action taken to prevent reoccurrence is to be published in ALB annual reports.

3.2.4 Development of NHS Information Governance capability and capacity, including Board Development

Building upon training needs analyses for Caldicott Guardians and other Information Governance staff conducted by DIP on behalf of the UK Caldicott Guardian Council in the autumn of 2007, an Education Training and Development (ETD) plan was developed. The analyses identified three generally preferred methods of receiving IG awareness, introductory and refresher training:

- Centrally provided e-learning
- Centrally provided workshops
- For Caldicott Guardians, a National Conference

During May 2008 the first phase (six modules) of an IG e-learning tool was launched. The initial focus was on introductory materials aimed at all NHS staff, but over the next year it will expand to provide a structured e-learning programme with Introductory, Foundation and Practitioner level modules. The tool provides for staff assessment and report generation, so it is capable of supporting induction process, annual training and refresher training. Initial feedback has been positive and plans are now in place for further development over the coming 12 months. This will include a module for Board members. A decision will need to be taken by Ministers in respect of mandating annual training for all NHS staff, as now required of all central government staff. (see section 6.1.11)

A series of workshops have been planned, eight for each SHA region, for the second half of 2008/9. These will focus on primary care.

The UK Caldicott Guardian Council has agreed to host a National Conference in London, February 2009. Plans and the agenda are being drawn up.

Most health communities have local IG networking groups to support and provide focus for their work. Additionally an SHA IG network has recently been established. The group is chaired by the SHA CIO Forum member that holds the Information Governance portfolio; this is currently the SHA CIO for East of England. Membership is drawn from each of the 10 SHAs. Each SHA member will be responsible for ensuring that the SHA has mechanisms in place to cascade IG communications to relevant staff in all providers in the health community, and this will include local IG networking groups. The first formal meeting will be held in June and monthly thereafter. The Terms of Reference are currently being agreed.

3.2.5 Specification of, and support for, encryption standards and tools for use with sensitive person identifiable information

Encryption Tool

A central procurement of an encryption tool was undertaken, with the tool being available for download from 20 March 2008. This has provided the organisation with a tool for the encryption of hard disks and removable media. The implementation of this tool across the organisation is now underway (where individual organisations had not already implemented solutions or are choosing to replace those with this tool).

The overall status of encryption implementation appears to be that it is on track, but that it is taking far longer than anticipated. Understandably, organisations are planning deployments carefully and ensuring that the impact of change is minimised. Many organisations have indicated that they are aiming to have completed their deployments by the end of the year.

There is clearly a need to ensure that all organisations have a robust approach to managing information risk in the interim and that Trust Boards are alerted to and take ownership of any risks that need to be accepted in order to deliver care.

A key finding of the analysis is that whilst some organisations had already implemented or begun implementation of encryption, the trigger for many was the central mandate of encryption. For the majority of these, progress on implementation has been dependent on the availability of a centrally procured solution and technical support from the supplier.

The adoption of the centrally procured McAfee products is not universal and many organisations have existing implementations of various technologies, which typically have been chosen due to their integration with existing estate infrastructure and processes.

Secure Bulk Transfer

A mechanism for the secure transfer of bulk data (greater than 20MB) has been devised, implemented and a pilot commenced. This pilot will run until the end of July and, providing the resultant evaluation is successful, will then

be made more widely available. The ongoing responsibility for this activity is set out in section 6.

Encryption of GP Backup Tapes

Activities have taken place to establish solutions for the encryption of backup tapes from GPSoC suppliers. Requirements have been produced, issued to suppliers, and they have responded. Agreement has been reached with three suppliers and the services are now available for ordering. Agreements with the remaining suppliers are still in the process of being finalised and will be published on the GPSoC website as these are agreed.

3.3 Integration with Governmental and wider reviews.

3.3.1 Review of the overseas processing of person identifiable information

Guidance has been developed, but before this can be finalised and published there is significant negotiation and co-ordination required with Cabinet Office and other Government Departments. This will therefore not complete within the timescale of this programme, but will be taken forward by Digital Information Policy (see section 6.1.5).

3.3.2 DH liaison/response to Cabinet Office Data Handling Review

DH has maintained close contact with the Cabinet Office throughout the review, reporting breaches and responding to information requests in line with our obligations, and in addition also:

- Taken part in “Red Team” reviews of reports and guidance in preparation;
- Shared the experience of developing and implementing the NHS Information Governance Toolkit and linked on-line learning resources;
- Helped the Cabinet Office assess options and requirements for a common on-line learning package for data handling;
- Challenged and engaged the Cabinet Office on timescales, to take account of the realities of effecting change in the NHS;
- Contributed speaker(s) for Cabinet Office workshops and conferences, with an extended leadership role on training and on-line support and a case study presented at the Information Assurance 08 conference in June.

Well-established contacts are in place between the Cabinet Office Data Handling Team, DH, and NHS CFH to ensure effective cooperation as further elements of the strategy are implemented and embedded.

The requirements of the Cabinet Office Data Handling Review have been incorporated within the Information Governance Toolkit, as far is practicable for citizen facing services. A report has been prepared to inform the Cabinet Office about how the NHS will manage information risk in line with public sector requirements (see section 6.1.11).

3.3.3 Data Sharing Review

On 25 October 2007, the Prime Minister asked Richard Thomas, the Information Commissioner and Dr Mark Walport, Chief Executive of the Wellcome Trust, to undertake a review of the framework for the use of personal information in the public and private sectors. This review took place alongside the Cabinet Office Data Handling Review and reported on 11 July 2008.

The SRO of the Information Governance Assurance Programme and a number of supporting officials were invited to contribute to the review, and the Digital Information Policy Branch submitted a response on behalf of the Department of Health.

The Report of the review was aligned with and reflected the Cabinet Office Data Handling Review, but concentrated on the legal and regulatory framework. At the time of writing the Government has not yet published its response to the recommendations in the report, some of which were NHS specific, but an analysis by the Digital Information Policy Branch concluded that the recommendations would have no direct impact on IGAP's own recommendations and were generally complementary to the direction of travel established by the IGAP.

4 Achievement of Programme Objectives

The specific objectives of the Information Governance Assurance Programme, as stated in the PID (*ref 2*) were:

1. to provide comprehensive assurance around current policies and practices around the secure and confidential management of sensitive person identifiable information by March 31st;
2. to provide frequent and not less than annual external assurances around confidentiality and security of sensitive person identifiable information to their key stakeholders and audiences;
3. to ensure that organisations have robust and effective IG policies and processes of equivalent stature to, and where appropriate are integrated with, those for corporate, clinical and financial governance.

During the course of the programme guidance was issued by Cabinet Office to all Government Departments containing minimum standards to be achieved regarding data handling, along with a timetable for implementation. These aligned with the existing objectives of the programme, and the required activities and milestones were incorporated into the programme plans. The DH and its ALBs will broadly adhere to the targets set by the Cabinet Office. It is important to note however, that the requirements and timetable differs for customer facing services such as the NHS. The approach in respect of the NHS is described in section 6.1.11. For the purposes of this report, the implementation of the Cabinet Office guidance where required and the minimum standards therein, has been taken as an additional programme objective.

4.1 Objective 1 – Assurance by 31/03/08

When the programme commenced in February 2008, work had already been initiated to achieve the required assurances by 31/03/08. The programme inherited these activities, incorporated them into the programme plans and monitored their completion. The activities were separated into various groupings to reflect the different parts of the organisation. The results of each of these are as follows:

4.1.1 DH & NHS CFH

Information management risk has been established as a corporate risk to be considered by the Audit Committee and at Board level, and built into existing assurance arrangements. Progress was reported to the DH Audit Committee in March and June 2008.

4.1.2 Arms Length Bodies

Assurance for IGAP has been built into the existing assurance arrangements for ALBs. ALBs are reporting their progress to their Senior Departmental Sponsors in DH as part of the 2007-08 quarter four accountability review meetings.

4.1.3 NHS

The quality of the responses from the individual SHAs has been variable in terms of depth and detail provided, but all evidenced the significant effort in the development of action plans and investment in the data mapping, risk assessment and mitigation across the various health communities. Many of the Trusts have provided assurances that are caveated to a degree.

4.1.4 Foundation Trusts

Monitor has independently sought assurance from Foundation Trusts. This assurance has been informed by the Cabinet Office mandated actions, and where FTs were unable to provide full assurance Monitor has set clear expectations about responsibility for action.

4.1.5 Centrally Contracted Independent Sector Providers

Independent Sector (IS) providers centrally contracted through the ISTC Programme have completed the IG toolkit and IG Statement of Compliance, in accordance with standard NHS CfH practice. However, additional assurance has been sought from provider chief executives with respect to the 16 NHS core standards in accordance with assurances previously sought from SHAs. All sixteen IS providers have responded, with a mixture of unqualified and qualified assurances being received. Key issues raised in the responses include offshore data processing, mapping of information flows, encryption and policy development. All providers either have, or are working towards, ISO 27001: Information Security Management certification and have given commitments to rectify qualifications to their assurance.

4.2 Objective 2 – Ongoing Assurance

The programme has developed an Information Governance Assurance Framework (see sections 3.2 and 8.1) which encompasses the various components that already existed and have been enhanced during this programme, as well as some new components. The IG Assurance Framework does require further work beyond the end of the programme and this is set out in section 8.1.

The programme has delivered:

- An online IG Training Tool;
- The establishment of training sessions for PCTs over the coming 12 months;
- Revisions to the IG Toolkit to reflect Cabinet Office materials;
- Revisions to annual reporting processes to meet Cabinet Office requirements and provide for greater visibility and accountability of sensitive person data related incidents;
- Revisions to the Statement of Internal Controls to include Information Governance;
- A centrally procured encryption tool;
- A pilot solution for bulk data transfer;

- Services for the encryption of GPSoC backup tapes.

This then provides mechanisms for organisations to ensure that they can both hold information securely and transmit it securely when necessary. The implementation and use of the mechanisms is down to individual organisations, but recommendations are made in section 8 as to how arrangements within the Department of Health could be strengthened to aid this process.

4.3 Objective 3 – Robust IG Policies and Procedures

As part of the development of the IG Assurance Framework, a “Standard” has been developed that documents in high-level terms the standards that all organisations within the enterprise have to meet. This was derived from and aligned with the NHS Information Governance Toolkit v6, and will be familiar to those organisations that have been working with the toolkit. This is covered on three pages and hence is something that can be used with boards/senior management teams to make clear their responsibilities with regard to Information Governance. This, supported by the interpretation of these standards for individual organisation types, guidance on what these mean and how they should be implemented, means that the implementation of IG policies is now on a much more robust footing.

Organisations are now required to include Information Governance issues in Untoward Incident reporting processes and in Annual reports. This will improve the transparency of reporting such incidents by bringing them into public forums. In addition, the inclusion of these issues in the Statement of Internal Control will mean personal involvement of Chief Executives on a regular basis, much greater non Executive Director input, and routine audit of internal processes in all organisations.

As far as possible, all providers of NHS services are being brought into the same Assurance Framework. Independent Sector providers already have strong contractual commitments to Information Governance provisions, including the use of the IG Toolkit, and have gone through the same compliance process as NHS organisations undertook at the end of 2007/08. The contractual provisions for independent sector organisations are currently being reviewed to bring them into line with the provisions of the Assurance Framework that the NHS Chief Executive has laid out for the NHS.

The programme has also worked with Monitor to ensure that Foundation Trusts are required to meet the same standards as other organisations, again ensuring consistency across all providers of NHS care.

4.4 Objective 4 – Implement Cabinet Office Minimum Standards

The Cabinet Office published the outcome of the Data Handling Review on 25 June 2008, but in advance of publication they provided Departments with a set of minimum standards to handle information risk and asked them to implement these as soon as possible (letter from Sir Gus O’Donnell to Permanent Secretaries dated 6 March 2008). These standards also have target completion dates associated with them, which are:

- 1 April 2008;
- 1 July 2008;

- By the end of the second quarter 2008/2009;
- During 2008/2009.

The DH, NHS CFH and the Arms Length Bodies have completed all the actions required by 1 April 2008. All of the actions required by 1 April 2008 have been completed within the NHS with the exception of the nomination of a Senior Information Risk Owner, although they have been informed of the need to nominate one, but further guidance on this has been issued in version 6 of the IG Toolkit.

The actions required by 1 July 2008 have not all been met within the DH and NHS CFH, as this timescale is not realistic for some of the activities. As regards the NHS, a separate piece of work is underway to establish how and when the various standards will apply to the NHS (see section 6.1.11). Most ALBs are expected to have completed the majority of the actions, and ALBs will have an action plan in place for the delivery of any remaining actions.

Some of the longer term actions also have similar issues, but section 6 identifies where the ownership of the implementation of all these outstanding activities lies.

5 Benefit Realisation

The intended benefits of the programme, as set out in the PID (*ref 2*) were:

1. Assurance to the general public, staff, key stakeholders and Ministers that person identifiable information is managed securely and confidentially.
2. Enhanced security of information flows and transfers of person identifiable information within the NHS and supporting organisations.
3. Increased awareness and profile of Information Governance within provider and support organisations with regard to handling sensitive person identifiable information.
4. Improved reputation for the Department of Health and NHS and potentially reduced likelihood of litigation.
5. Improved ability to hold individuals accountable for their responsibilities.

The PID stated that the realisation of the benefits would be measured through:

- The increase in the number of organisations using the IG Toolkit;
- The number and severity of IG incidents reported through the SUI process over time;
- The percentage of organisations using the IG Toolkit that meet each of the individual standards in Appendix 1 to the PID over time.

5.1 Increase in organisations using the IGT

The number of organisations using the toolkit is not measurable on anything less than an annual basis, when annual returns are submitted. Therefore, the expectation is that there will have been an increase as a result of the programme, but this cannot be verified until after 31/03/09. The baseline figure for the number of organisations using the toolkit is 5641 at 31/03/08. All drivers underpinning future increase in the IG Toolkit use are now incorporated in the Information Governance Assurance Framework and will be monitored annually.

5.2 Number & Severity of IG SUIs

The Serious Untoward Incidents (SUIs) in respect of Sensitive Person Identifiable Information (SPII) that have been reported between 1 December 2007 and 31 May 2008 have been collated and analysed. The categorisation of person identifiable information SUIs was set out in a letter to NHS Chief Executives in February 2008; hence, some of the categorisation undertaken here has been retrospective.

Figure 1 shows the number of SPII SUIs that have been reported monthly along with a breakdown of the number in each category. A 6-month snapshot of such data is too short to draw any firm conclusions on trends, but a more meaningful analysis can be conducted in 6 or 12 months time as there will then be more data available to draw conclusions on trends and the impact that this programme has had.

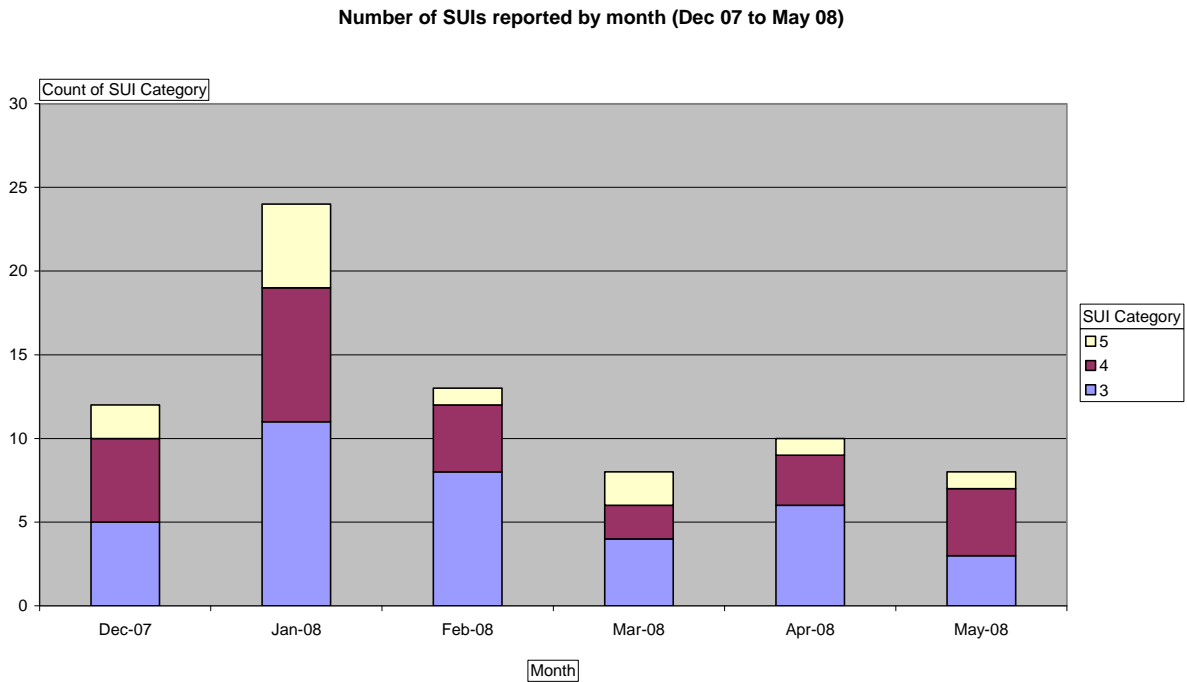


Figure 1

Further detail on the analysis of these SUIs is provided in Appendix 1.

5.3 Percentage split on scores for the 16 standards

The analysis of scores for organisations using the toolkit can only be measured on an annual basis, when annual returns are submitted. However, the baseline figures (from March 08 returns) for the average percentage split of scores on the 16 standards, compared with average across Statement of Compliance standards for 06/07 (broadly comparable), is set out in the following table: There is a marked improvement in performance for PCTs and SHAs that can be directly attributed to the Information Governance Assurance Programme. The impact of the IGAP will also be reflected in toolkit returns submitted in March 2009.

Organisation type	Average attainment across 16 standards 07/08	Percentage (score of 3 = 100%)	Average attainment across Statement of Compliance standards 06/07	Percentage (score of 3 = 100%)
SHA	2.05	68%	1.39	46%
Acute Trust	2.32	77%	2.24	75%
Ambulance Trust	2.23	74%	1.91	64%
MHT	2.42	81%	2.17	72%
PCT	2.27	76%	1.88	63%

The above table does not include other organisation types (e.g. Arms Length Bodies) as the take-up and use of the IG Toolkit is not currently widespread within those organisation types.

6 Handover and Transition Activities

6.1 Incomplete Activities

This section sets out those activities/milestones on the plan that are either under way or have not yet started, detailing why they have not completed and how the owner is going forward.

6.1.1 GPs, Dentists, Pharmacies & Opticians (independent contractors)

A strategy has been developed, in the form of a negotiated roadmap, to bring pharmacies into the Information Governance Assurance Framework. Negotiations have started with the representative body, and the initial phase of mapping the IG standards to the existing Pharmacy contract and legislation has been completed. This represents a significant change for small organisations and they will need to be supported with training kits, workshops, advice, helplines and possibly some funding to eradicate unacceptable working practices such as modems connected to N3 workstations. It is proposed that other similar groups including opticians and dentists will be approached with a similar strategy.

Recommendation 4. *Work should be undertaken to formally bring independent contractors into the IG Assurance Framework as soon as is practicable.*

Health Ministers have also asked for options for strengthening the IG requirements in the GP contract to be explored.

Recommendation 5. *Options for changes to the GMS contract should be considered at the earliest available opportunity.*

6.1.2 Arms Length Bodies

The ALB Business Support Unit in DH will continue to coordinate arrangements for the ALBs to meet the outstanding Cabinet Office requirements. The existing performance management arrangements of quarterly accountability review meetings between ALB CEOs and the DH Directors-General who are their Senior Departmental Sponsors will be used to provide assurance. Work also needs to continue to identify accountability arrangements for all bodies and to bring them within the Information Governance assurance Framework.

Recommendation 6. *Work should be undertaken to formally bring all ALBs into the IG Assurance Framework by 01/04/09.*

6.1.3 Embed in Annual Reporting Processes & Procedures

Instructions have been issued regarding the contents of annual reports and the annual Statement of Internal Controls (SIC) in line with the Cabinet Office requirements (see section 3.2.2). These instructions relate to 2007/08 and future years - however, the intention of these activities was to ensure that these instructions were embedded in the relevant Financial Manuals and associated guidance. The NHS 08/09 Manual of Accounts will be issued in draft form at the end of June for consultation prior to finalisation. This draft

will reflect the new requirements of the Annual Report. The draft guidance to accompany the Manual will be published later in the year reflecting, in part, the consultation and make clear the explicit need to reference IG in the SIC, the wording reflecting closely that used by the Cabinet Office in relation to Government Departments. There will also continue to be a need to liaise with Monitor regarding the Financial Reporting Manual for Foundation Trusts. The responsibility for ensuring that this completes satisfactorily will lie with the Access Controls Team within NHS CFH.

Recommendation 7.	<i>The NHS Manual of Accounts for 08/09 and thereafter and its associated guidance should be amended to reflect IG requirements.</i>
--------------------------	--

6.1.4 Development of NHS Information Governance capability and capacity, including Board Development

Arrangements have been established for the delivery of 80 IG workshops across the SHAs aimed at PCT and GP Practice staff. The detailed planning and subsequent delivery of these will be the responsibility of the Department's Digital Information Policy Branch, who will be commencing with pilots during July 2008.

Further work will be undertaken by Digital Information Policy Branch to support the development of NHS Information Governance Education Training and Development (ETD), in particular the online IG Training Tool.

Recommendation 8.	<i>IG Education Training & Development should be further developed to reflect the requirements of the NHS and other users.</i>
--------------------------	--

Recommendation 9.	<i>Two new national groups should be established: a National IG ETD Reference Group; and a National IG ETD User Group.</i>
--------------------------	--

Guidance for NHS Board Members: Health Informatics 2008

This paper was first published in 1998, by the NHS Information Authority, and updated in 2002. It is to be reissued later this year by NHS CFH with a foreword from the NHS Chief Executive, and has been revised to include detailed reference to the Information Governance Assurance Framework. It is aimed at a broad audience, including Chairs, non-executive directors and senior staff involved in informatics.

Integrated Governance Handbook

This handbook is targeted at Executive and non Executive Directors of NHS Boards, and is intended to aid them in delivering their responsibilities for integrated governance. The NHS Confederation is currently producing an adjunct to the Handbook specifically around Governance between organisations, which is particularly pertinent in respect of information governance. The team undertaking the work has launched (20th June) a discussion paper prior to a formal update of guidance later in the year. In discussion, that team have indicated a willingness to ensure IG is reflected in their work and will require ongoing consultation until the autumn. This will be a further means of ensuring that IG is perceived as a Board level issue,

requiring integration with other strands of governance, notably financial and clinical.

Recommendation 10. *The work required to embed Information Governance within the Integrated Governance Handbook should be concluded.*

More general guidance is also required for Boards on Information Governance requirements and their responsibilities, not only as a resource for Board members but also to underpin training provision for them.

Recommendation 11. *Further work should be undertaken to ensure that IG is referenced appropriately in guidance for Boards.*

6.1.5 Overseas Processing of Person Identifiable Information

Work is required to establish a clear policy, endorsed by the Information Commissioner and aligned with Cabinet Office guidelines for the public sector, on when it is appropriate to permit patient information to be processed outside of the UK. This policy must be supported by guidance that enables appropriate decision making by the Department of Health and its ALBs, the NHS and partner organisations, and provides a clear indication of the safeguards that need to be in place to protect the interests of patients

Recommendation 12. *Further work should be undertaken to develop guidance on overseas Processing of Personal Data.*

6.1.6 Healthcare Commission

The Information Governance Assurance Programme engaged productively with the Healthcare Commission to discuss the assessment of core healthcare standards for 2007/8 and 2008/9. Although the assessment criteria had been published for 2007/8, agreement was reached on the approach to be adopted by assessors when looking at aspects of secure data handling, which would provide greater assurance than was previously the case. Work is required to set new assessment criteria for 2008/9 and the Healthcare Commission has committed to working with the Department's Digital Information Policy Branch to deliver this revised approach.

Recommendation 13. *Further work should be undertaken to ensure that the Healthcare Commission's assessment criteria appropriately reflect IG requirements.*

6.1.7 Review of Resource Requirements

A review of Information Governance resource requirements across the NHS was conducted by the Department's Digital Information Policy Branch, in collaboration with the UK Council of Caldicott Guardians and the Medical Manager's sub-committee of the BMA. The report of the review will be published shortly after the termination of the IGAP but its findings were inconclusive, reflecting a lack of coherency and understanding in NHS bodies. Further work is being commissioned by Digital Information Policy to review the relationship between resources and performance in a range of high and low achieving organisations.

Recommendation 14. *Further work should be undertaken to develop and consult on guidelines for effectively resourcing IG for different organisation types*

6.1.8 Secure Bulk Data Transfer

A pilot of a solution for the secure transfer of bulk data is underway (see section 3.2.5). This is scheduled to complete at the end of July 2008 with an evaluation prior to the consideration of the options for widespread use. The target is to have a solution available for use by all organisations by 31st December 2008. This will be taken forward by the NHS CFH Infrastructure Security Team.

Recommendation 15. *Further work is undertaken to ensure that a nationally available solution to the secure transfer of bulk data is available for use by 31st December 2008.*

6.1.9 Registration Authorities

An underpinning principle of the IG Assurance Programme has been that there should not be any differentiation between providers of NHS services in terms of the principle or practice of Information governance. Currently independent sector organisations providing NHS services rely on the Registration Authorities within NHS organisations (mainly PCTs) to manage access controls for their staff using NHS CRS applications. This is principally for C&B and SUS at the moment, but the use of other applications will become more extensive. Unlike NHS providers, independent sector providers do not carry the responsibility for this important aspect of governance control, and therefore this IGAP principle is undermined.

In addition, there are major logistical issues of complexity with the Registration Authorities (RAs) within PCTs having to handle the access of individuals within IS organisations, which are so severe that governance risks are created. Application of this principle in this regard would therefore strengthen governance in practice.

Independent sector organisations are already subject through the Statement of Compliance and the contractual framework to many governance controls including IGT returns, and the contractual provisions are being extended to incorporate all relevant sections of the IG assurance framework.

Both the Care Record Development Board and the National Programme Board Executive have approved the principal of RAs being established in those independent sector organisations who, on application to CFH to establish a RA, can demonstrate need, an appropriate infrastructure to support it, and the required governance policies and procedures embedded within the organisation. The approval process will stipulate the quality assurance and monitoring and audit process.

To meet the IGAP principal of consistent treatment of all NHS providers, independent sector providers of NHS services should therefore be permitted to assume responsibility for the management of access controls for their staff needing to access NHS CRS applications, by establishing RAs according to strict criteria outlined above.

Recommendation 16.	<i>Independent sector providers of NHS services should be permitted to assume responsibility for the management of access controls for their staff needing to access NHS CRS applications by establishing Registration Authorities according to strict criteria.</i>
---------------------------	--

6.1.10 Confidentiality and Disciplinary Policies

The DH Workforce and NHS Employers have agreed a joint review of policy and guidance around staff confidentiality and Disciplinary policies in the NHS. This is designed to ensure that all NHS organisations are consistent in the treatment of staff involved in incidents of data security and confidentiality breaches. A dialogue on the same subject has been opened with the professional regulators. The expected outcomes are clarification and confirmation of the expectations of NHS organisations in these policy areas, to include a higher degree of transparency in dealing with such issues and to provide greater public confidence in the NHS to store securely and use safely their personal data. It is expected to complete the work with NHS Employers in July, and the work with the professional regulators in the autumn.

The intention is that IG SUIs will be investigated in line with other SUIs, using recognised techniques, such as root cause analysis, which are designed to identify all the relevant factors (organisational and individual). Individuals will be treated fairly and in accordance with HR policies and professional codes of conduct.

The recommendations for the NHS will inform the guidance to be issued to the ALBs for amendments to their HR policies.

Recommendation 17.	<i>Further work is undertaken to complete the review of confidentiality and disciplinary procedures</i>
---------------------------	---

Recommendation 18.	<i>Further work is undertaken to ensure that the ALBs have a consistent approach in their organisations regarding confidentiality and disciplinary policies.</i>
---------------------------	--

6.1.11 Implementation of Cabinet Office Requirements

Many of the Cabinet Office requirements have target dates for implementation that are beyond the end of this programme, and hence these will all be carried forward by the relevant group as identified below.

The DH has action plans in place to address the Cabinet Office requirements, although some of them may not be achieved in accordance with the timescale set by Cabinet Office. These will be taken forward by Information Services within DH. Achievement of the Cabinet Office requirements by the Arms Length Bodies will be monitored and progressed by the ALB Business Support Unit within DH.

The approach with respect to the NHS is necessarily different and has been considered and agreed with the National Information Governance Board. Many of the Cabinet Office requirements relate to industry standard security measures, and these are generally as applicable to the NHS as to central government. Requirements that fall into this category have been included in version 6 of the IG Toolkit. Other requirements, e.g. accreditation of IT

systems to central government standards, are not applicable for customer facing services where the business needs are very different. There is a third category of requirement, e.g. mandated training for all staff annually, which might be desirable for the NHS but which have significant resource implications which need to be considered by Ministers.

<p>Recommendation 19. <i>Further work is undertaken to inform the Cabinet Office and Ministers about the approach proposed for meeting the Cabinet Office requirements in the NHS and to seek Ministerial agreement where there are issues of practicality and/or resources.</i></p>

6.1.12 Standard NHS Contracts and Central Independent Sector (IS) Contracts

Centrally let Independent Sector (IS) contracts require review and amendment to ensure they reflect the requirements of the Information Governance Assurance Framework and, where necessary, clarify Data Controller responsibilities. Broadly, the window to do this is between October and April each year and this work will be led by the Performance Management and Operations Directorate.

The Standard NHS contracts also need to include appropriate reference to the Information Governance Assurance Framework. Changes to the Acute contract and content of the new Mental Health and Community contracts need to be flagged as part of the NHS Operating Framework and therefore need to be complete by October. This work will also be led by the Performance Management and Operations Directorate.

<p>Recommendation 20. <i>Further work is undertaken to ensure that both the central IS Contracts (by April 2009) and the Standard NHS contracts (by October 2008) include appropriate reference to the requirements of the Information Governance Assurance Framework</i></p>
--

6.2 Risks and Issues

The programme's risk and issue log can be found in Appendix 4. This shows the status of all the risks and issues at programme closure. Any risks or issues which cannot be closed have been annotated with the organisational group(s) and the individual that will own the risk/issue following programme closure.

6.3 Transition Activities

The closure of the Information Governance Assurance Programme means that there is potential for momentum to be lost in relation to the recommendations provided in this section, whilst the recommendations in section 8 of this document are agreed and implemented. The executive team brought together in support of IGAP has effectively sustained momentum over the life of the Programme and has developed a collective understanding of what is required. It is well positioned to ensure the completion of residual work on behalf of the acting CIO for Health.

<p>Recommendation 21. <i>On behalf of the acting CIO for Health, the IGAP executive team (renamed as the IG Executive) should continue to meet on a fortnightly basis, in order to complete any residual actions and transfer to business as usual activity, chaired by Philip Brown with support from DIP. This to be reviewed at the end of October.</i></p>

7 Programme Documentation

All of the programme documentation is currently on a SharePoint site hosted by NHS CFH. At the end of the programme, the contents of this site will be archived to CD and the SharePoint site deleted.

The information held and which will be archived to CD is set out in the following table:

Folder	Contents
Background Documents	Documents relevant to the programme created prior to the programme.
Cabinet Office	Materials issued by Cabinet Office.
Communications and Stakeholder Engagement	Communications plan and all communications issued by the programme.
Encryption Tools	Information relating to the encryption tools including feedback received from SHAs on deployment.
IG Assurance Framework	Documents relating to the development of the framework.
Independent Sector	Documents relating to the Independent Sector.
Minister	Ministerial submissions made in relation to the programme.
Organisations in scope	Documents relating to the DH work undertaken to define the organisational relationships and accountabilities.
PID	The Programme Initiation Document.
Plans	The Programme plans.
Presentations	Programme presentations.
Programme Board	Programme Board documents with a sub-folder for each programme board meeting containing all of the papers for that meeting.
Programme Closedown	The programme closedown document.
Programme Executive	Programme Executive documents with a sub-folder for each programme executive meeting containing all of the papers for that meeting.
Risks and Issues	The programme risks & Issues log.
SUI analysis	Information received on Serious Untoward Incidents and the subsequent analysis.
Updates	Copies of the internal management updates provided to various bodies during the course of the programme.

Each member of the IGAP Programme Executive will be provided with a copy of the CD for future reference purposes and a copy will be lodged with the NHS CFH National Programme Office.

8 IG Assurance Framework and ongoing organisational structures

Section 3.2 sets out the work that has taken place to develop an IG Assurance Framework. This section details the further work and ongoing enhancement that will be necessary to ensure that the framework can provide the required assurance at all levels. The organisational changes required within the Department of Health going forward are also outlined, as are a number of similar pointers for the Department's Arms Length Bodies and for NHS organisations.

8.1 IG Assurance Framework

The Information Governance Assurance Framework consists of the following components:

National oversight

- National Information Governance Board

Central components

- Central Information Governance subject matter experts
- The Information Governance standard
- IG Toolkit; (which interprets the IG Standard for different organisation types and provides implementation guidance, reference materials and a performance assessment vehicle)
- IG Training provision
- IG Compliance mechanisms
 - Self Assessment reporting through the IG Toolkit
 - Information Governance Statement of Compliance
 - Audit processes

Local components

- IG Management Structures;
 - Executive Responsibility for IG;
 - IG Steering Group;
 - Caldicott Guardian (if applicable);
 - IG subject matter experts.
- Information Risk Management Structures;
 - SIRO;
 - Statement of Internal Controls and Annual Reports;
 - Incident Reporting;
 - Information Asset Owners.

The intention is that by 1st April 2009, these components will all be re-branded as the Information Governance Assurance Framework³.

Recommendation 22.	<i>The Information Governance Assurance Framework to be promoted as the collective brand name for all the components identified in section 8.1 with the launch to take place by 1st April 2009</i>
---------------------------	---

8.1.1 Ownership of the Information Governance Assurance Framework

The information Governance Assurance Framework is an enterprise wide asset that supports regulation and uniformity across the enterprise. As such, it should be owned by the CIO for Health, who should be advised by Digital Information Policy, the National Information Governance Board and other bodies where appropriate. An annual review of the Information Governance Assurance Framework should be conducted to ensure that it is fit for purpose along with the annual review of organisations' compliance. These should be overseen by the National Information Governance Board.

Recommendation 23.	<i>The CIO for Health should be the owner of the Information Governance Assurance Framework.</i>
---------------------------	--

Recommendation 24.	<i>The NIGB should oversee and report on the findings of an annual review of the national components of the Information Governance Assurance Framework and organisations' compliance.</i>
---------------------------	---

8.1.2 Intended Scope of the Information Governance Assurance Framework

The Information Governance Assurance Framework is intended to apply to all bodies that deliver or support the delivery of NHS services, including the Department of Health, its Arms Length Bodies, NHS bodies and organisations that provide or support NHS services under contract. All organisations within scope should work to the IG Standard, as provided in Appendix 2, and provide assurances through completion of an Information Governance Toolkit performance assessment.

Recommendation 25.	<i>All organisations delivering or supporting delivery of NHS services should be required to meet the Information Governance Standard and provide assurance through completion of an annual performance assessment through the Information Governance Toolkit.</i>
---------------------------	--

8.1.3 Minimum Standards of Achievement

The move to establish the Information Governance Assurance Framework needs to include firm targets for organisations to meet the key assurance requirements set out in the Information Governance Toolkit. There may need to be some flexibility in terms of deadlines set for organisations that are brought within the framework for the first time, but all organisation types should be set challenging, but achievable, targets for delivery.

³ It was not felt appropriate to do this during the life of the programme as the next version of the IG Toolkit was already in production, for issue at the end of June 2008. This will now take place when the minimum standards for the NHS have been agreed (see section 6.1.11) as these will require significant communication to the NHS and it is the NHS that will be mainly impacted by a change of name for the IG Toolkit.

Recommendation 26.	<i>Develop options for Ministers in respect of the mandate of specific levels of performance against key requirements in the information governance toolkit, including proposals for consultation on implementation timescales where appropriate.</i>
---------------------------	---

8.2 DH Organisational Requirements

8.2.1 Organisation Scope

The IG Standard (see Appendix 2) clearly sets out the responsibilities of “organisations”. Confusion arises when there are elements of the enterprise that may, or may not be, considered a separate “organisation”.

The Information Governance Assurance Programme has considered that:

- Each legally distinct NHS entity (e.g. SHA, PCT, Trust, GP Practice) is a separate organisation;
- Each legally distinct Arms Length Body is a separate organisation;
- Where bodies are not statutory they are part of the organisation that hosts/funds them and are not a separate organisation in their own right.

The conclusion from the above is therefore that the DH, as an organisation, includes NHS CFH and all ancillary bodies that are not statutory and are not hosted/funded by some other organisation within the enterprise.

8.2.2 Accountability & Governance

The Permanent Secretary for the Department of Health is ultimately accountable to Ministers for Information Governance across the Department of Health and its Arms Length Bodies. The newly created post of CIO for Health should be the Senior Information Risk Owner (SIRO) for the Department, or may report to him/her, but is appropriately positioned to be the focal point for Information Governance policies, standards and tools across the Department (including the NHS) going forward. This does not however take away the individual responsibility of DH Board members and NHS Management Board members to ensure that their parts of the organisation and associated delivery chains comply with the policies and standards.

Recommendation 27.	<i>The CIO for Health is accountable to the Permanent Secretary and the NHS CEO for the delivery and maintenance of the Information Governance Assurance Framework.</i>
---------------------------	---

The Senior Information Risk Owner for the Department needs to be supported by senior staff with appropriate responsibilities for managing information risk and for Information Governance.

Information Risk should be managed through the responsible officers identified below (Information Asset Owners) with the SIRO held to account by the Department’s audit committee and assurance provided through the statement of internal controls and the Annual Report.

Information Governance across DH should be managed through an Information Governance Steering Group, chaired by a “Senior Manager” (see the IG Standard, clause 3, which can be found in Appendix 2). It is recommended that the CIO (when appointed and in post) should identify a member of his/her management team to take overall responsibility for IG within DH. This individual should then be the chair of a Department wide steering group, with representatives from each of the core business areas. There may then be a number of subsidiary boards who have responsibility for specific DH information assets.

Recommendation 28.	<i>The CIO for Health should identify a member of his/her management team to provide leadership for IG in the DH and those bodies it hosts in IG terms (e.g. those ALBs which are not corporate entities).</i>
---------------------------	--

Recommendation 29.	<i>A Department wide Information Governance Steering Group should be established chaired by a senior manager with responsibility for IG.</i>
---------------------------	--

The Cabinet Office has mandated the roles of Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO) for Central Government Departments to provide a robust and consistent approach to managing information risk. These are also being required of the Department’s Arms Length Bodies and of NHS Trusts.

The DH SIRO must ensure that Information asset owners are determined for each of the assets held by DH (including all national NHS IT systems managed by CFH). These individuals must be senior staff accountable for, and with authority to make decisions about, the assets they control. Whilst operational responsibility for discharging the responsibilities of Information Asset Owners may be delegated to less senior staff, accountability must not be delegated inappropriately.

Recommendation 30.	<i>The DH establishes a single Information Asset Register covering the information assets in all its constituent bodies.</i>
---------------------------	--

Recommendation 31.	<i>The DH allocates Information Asset Owners for each of the Information Assets at a Director level.</i>
---------------------------	--

As a body that holds, through NHS CFH, a significant amount of confidential patient information the DH also requires an appropriately resourced and defined Caldicott Function, with the roles and support arrangements clarified and made transparent to staff. Any delegated authority to directorates (e.g. to CFH) should be clearly specified.

The relationship between the Information Risk Management structure, the Information Governance Management structure and the Caldicott function needs to be clearly documented.

Recommendation 32.	<i>The DH establishes an appropriately resourced Caldicott function and clearly defines roles, support arrangements and delegated authority.</i>
---------------------------	--

Recommendation 33. *The DH should clarify and document the relationships between the information risk management, information governance and Caldicott functions.*

8.2.3 Ministerial Reporting on Data Losses

While this programme has been in place much of the ministerial reporting regarding data losses throughout the entire organisation has been undertaken by the programme. This now needs to be established as a 'business as usual' function.

The NHS Business Unit within DH Performance Management and Operations Directorate is already established as the focal point for performance management issues arising within the NHS and the Independent Sector. This group should therefore take responsibility for any Ministerial reporting required in respect of data losses. In some cases they may require specialist advice in respect of particular data losses and this can be obtained from the DH CIO and their organisation (in respect of any IT related issues) and from DH Digital Information Policy as necessary.

Recommendation 34. *Ministerial reporting in respect of data losses within the NHS and Independent Sector should be undertaken by the NHS Business Unit*

It makes sense that all ministerial communications on data losses are undertaken by the same group, providing the Minister with a single point of contact for the entire organisation. The majority of the incidents are likely to occur within the NHS (as the largest portion of the organisation) and hence the NHS Business Unit is the logical choice as a single point of contact and co-ordination regarding data losses. There are however some issues to be resolved in establishing this, particularly in respect of Foundation Trusts.

Recommendation 35. *Establish a reporting mechanism for the DH and its entire delivery chain that aligns with the Cabinet Office and the Information Commissioner's requirements and public expectations.*

8.2.4 Relationships with other bodies

The Department of Health has, and needs to maintain, strong working relationships with a range of external bodies on information governance matters (e.g. the Cabinet Office, Other Government Departments, Monitor, Information Commissioner, Audit Commission, National Audit Office). As the individual accountable for IG to the Permanent Secretary and the NHS Chief Executive (see Recommendation 27) the CIO for Health must ensure that these relationships are adequately maintained. Current responsibility for these relationships is often shared between Digital Information Policy, NHS CFH and DH Information Services but there are common issues that suggest a more corporate approach would be beneficial.

Recommendation 36. *Strong working relationships should be developed to ensure that relationships with external bodies are managed consistently and effectively.*

8.3 NHS and ALB Organisational Requirements

8.3.1 Organisation Scope

In line with the Information Governance Standard provided in Appendix 2, it is particularly important that all organisations clearly understand all of the business areas that they are responsible for, whether these areas are core to the work of the organisation or just services hosted by the organisation under 'flag of convenience' arrangements. Assurances will be sought from organisations, that they are addressing the information governance performance of all in scope areas.

8.3.2 Accountability & Governance

Although it is not appropriate for a central specification of accountability and governance arrangements to be provided for all organisations, the Information Governance Toolkit provides guidance on key roles and on governance arrangements which, if followed, provide a basis for effective information governance.

Appendix 1 – Analysis of Sensitive Person Identifiable Information SUIs

Information on the Sensitive Person Identifiable Information (SPII) related Serious Untoward Incidents (SUIs) was requested from all SHAs for the period 1 December 2007 to 31 May 2008. This information has been analysed and the key findings are presented here.

Figure 2 shows the breakdown of the incidents by the primary media or device involved in the incident. The most significant observation from this is that almost 50% of the incidents involved paper rather than IT related items. This emphasises the fact that this is not an IT issue, but it is a general information issue and needs to be addressed in all aspects of the business, not just those that deal with information on IT devices.

As would be expected, the main device type involved in the IT related incidents are laptops. This is due to their inherent portability and also their attractiveness to thieves. The top five devices involved in incidents (Laptops, Memory Sticks, Back up tapes, CD/DVD, and Desktop PCs) have all been addressed by the Information Governance Assurance Programme as detailed earlier in this document.

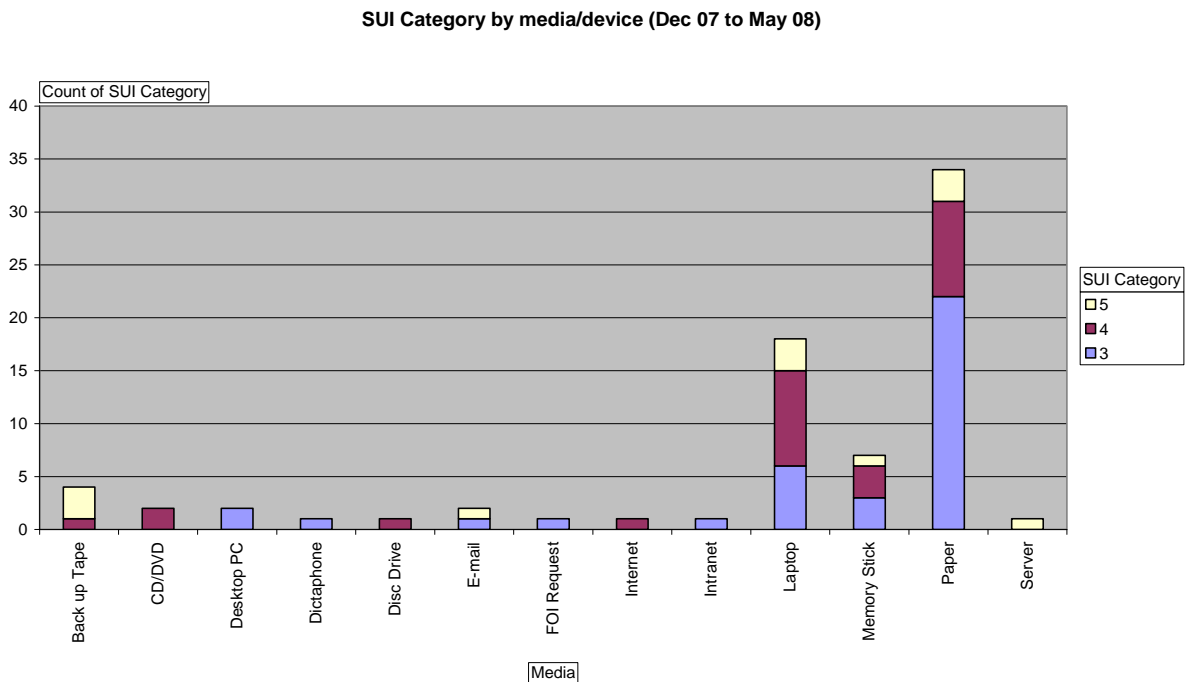


Figure 2

The analysis undertaken has also looked at the underlying (root) causes of the SPII SUIs that have occurred between 1 December 2007 and 31 May 2008. This analysis has come up with eight general categories of root cause:

- Confidential information inappropriately disclosed (e.g. staff given access to information which they should not have had access to);

- Inappropriate handling of confidential paper records (e.g. papers left on a train/bus);
- Insecure disposal of paper data (e.g. paper records found in a skip);
- Insufficient tracking of data/information assets (e.g. paper records lost or left behind during office moves);
- Physical device failure (e.g. letter insertion machine inserting letters into the wrong envelopes);
- Transfer of unencrypted data by an insecure mechanism (e.g. sending unencrypted back up tapes by normal courier);
- Unencrypted data on a device at risk of theft (e.g. unencrypted data on a desktop PC or laptop even though on NHS premises);
- Unencrypted data taken off site (e.g. unencrypted data on a laptop or memory stick).

Figure 3 shows the breakdown of the SUIs in this period by their underlying root cause.

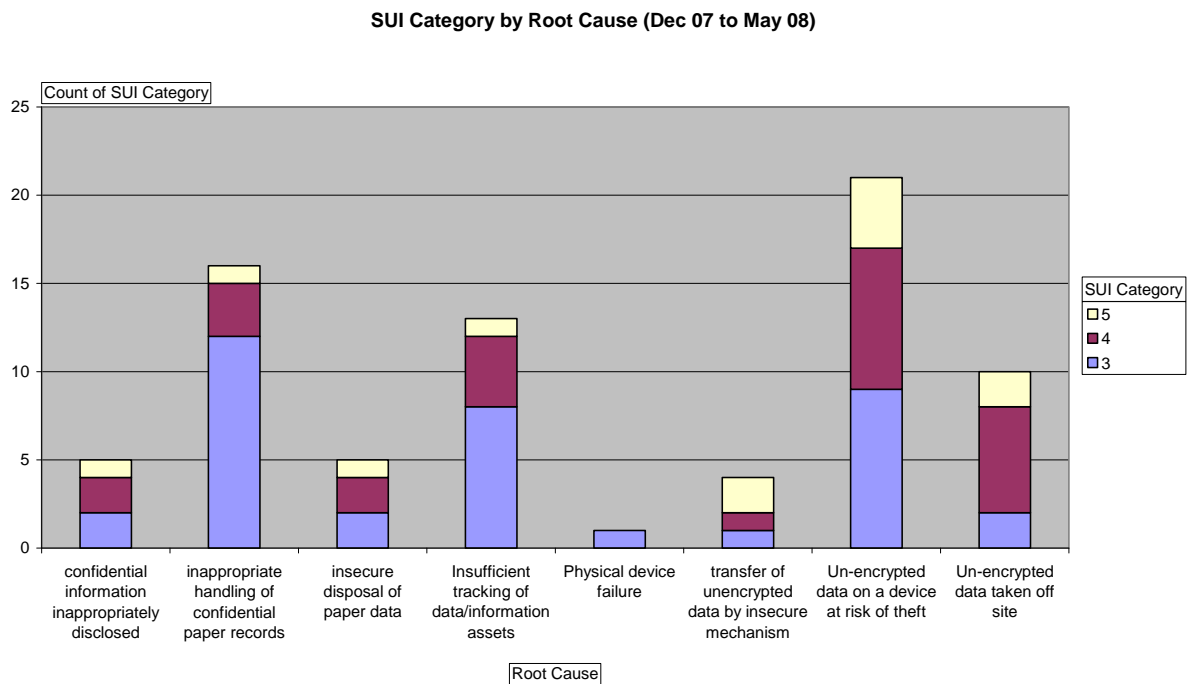


Figure 3

There are a number of key learning points that have been derived from the analysis of this data:

- All devices holding Sensitive Person Identifiable Information should be encrypted

It is clear that devices that are taken out of the office should be encrypted, to protect not only against theft, but also loss. However, it is also clear from the analysis that most IT devices are at risk of theft, even if they are on NHS premises and even if they are kept in locked offices or even locked filing

cabinets within locked offices. The only way to mitigate this risk is to encrypt the data.

- Check that the information being disclosed: a) is only that which was requested b) does not contain inappropriate data

There have been a number of incidents where there has been a legitimate request for information, but then the process to supply that information has broken down. This may be because incorrect information is being sent (e.g. the data for a different GP practice than that requested) or, particularly where the request may be quite broad as in an FOI request, by failing to ensure that the information does not include person identifiable information.

- confidential waste should be treated with the same seriousness as clinical waste

Whenever paper records that contain person identifiable information need disposal, then this needs to be done in a secure manner. Within the NHS there already exists a clearly understood culture for the secure disposal of clinical waste. Confidential waste should be treated with the same seriousness. A number of the incidents analysed related to paper records being found in inappropriate waste containers.

- Emphasise the message that confidential information in the possession of an individual should be treated as a large amount of their own cash

There have been many incidents where staff have legitimately had paper records in their possession in order to undertake their job (either in or outside NHS premises), but the individuals have then lost or mislaid them in public places. The message that individuals should treat confidential information in their possession as a large amount of their own cash has already been given, however, it is important to keep promoting this message.

- Encrypt all sensitive person identifiable information when in transit

There have been a number of examples of data being moved between individuals/organisations for valid reasons, but using insecure mechanisms (usually because that is the only mechanism available). By their very nature these insecure mechanisms sometimes fail resulting in the loss of the data. While some of the mechanisms used can be replaced by secure mechanisms, the most cost effective way of dealing with many of them is to encrypt the data such that if loss does occur, it will have minimal impact.

- Ensure individuals only have access to the information they require to do their job and are appropriately trained

There are strong controls on many IT systems to ensure that access is restricted to only those individuals who need particular information. However, paper records are sometimes more easily accessible and individuals may be involved in filing or archiving of these records without necessarily understanding the confidential nature and the responsibilities associated with that.

- Ensure items are correctly addressed and receipt should be acknowledged and followed up if not received.

When paper based information has to be transferred between organisations/individuals it cannot be encrypted as with electronic data. Greater care therefore has to be taken in making sure that the item is correctly addressed, that the receiver knows it has been sent and that the receiver provides a positive or negative acknowledgement to its receipt.

- Ensure you know where information is expected to be received from and follow up when it does not arrive.

If an organisation validly requests confidential information from others (which may be outside the NHS) then it should ensure that it knows exactly who should be providing information and take positive steps to follow up non-receipt.

- Machines handling confidential information should be treated in the same category as those with patient safety implications

Where a machine is used in the transmission of confidential paper based information (e.g. a letter insertion machine) it must be recognised that it may fail and needs to be tested and maintained in the same way that a machine with patient safety implications would be.

- Make couriers aware of the nature of the information being transferred. Courier companies should treat confidential information as a large amount of their own cash.

When paper based information has to be moved via couriers it cannot be encrypted as with electronic data. The courier companies should therefore be made aware of the nature of the data they are carrying and as with staff; they should be treating the information as a large amount of their own cash.

- Refurbishment/moves are high-risk activities for preservation of information assets.

There have been a number of occurrences where paper based data or PCs etc. have been mislaid during office re-locations or refurbishments. It should be recognised that these are high-risk activities and hence extra care needs to be taken to preserve information assets at these times.

Appendix 2 – IG Standard (draft)

This appendix contains the draft IG Standard as developed by the programme. The intention is that this is a high-level statement of the requirements placed on all organisations within the enterprise (including DH itself), and forms the high-level component of the IG Assurance Framework. This will be further progressed through the appropriate standards bodies to achieve recognised status as a standard.

IG Standard

This framework standard provides a consistent basis for robust information governance for all organisations that provide or support NHS or social care services (including the Department of Health and its Arm's Length Bodies). This embraces a wide range of organisation types and the detailed guidance on how to apply the framework needs to reflect the differences between organisations. This guidance is provided through the Information Governance Toolkit, which can be accessed according to organisation type.

Management & Accountability

1. All organisations must have robust management and accountability arrangements for all aspects of Information Governance. What this means in practice for the different organisation types is described in the Information Governance Toolkit. These arrangements must be annually reviewed by the senior management team to ensure compliance.
2. All organisations' senior management teams must sign-off an annual Information Governance Performance assessment and, where required, produce a Statement of Internal Control (SIC) and an Annual Report that appropriately reference information governance performance in respect of the organisation itself and any contracted services.
3. All organisations must have an Information Governance Steering Group, or equivalent, chaired by a senior manager and must have access to appropriately skilled expertise across the entire Information Governance agenda.
4. All organisations that process identifiable service user data must have an appropriately supported Caldicott function.
5. All organisations must assign appropriate responsibilities for information governance to staff according to their roles.
6. All organisations must establish a register of all major information assets and assign responsibility or 'ownership' for each asset. Lesser information assets should be managed through local policy and procedure.
7. All organisations must ensure that information risks are identified and managed, where applicable, through its network of local 'owners' of information assets. Information risk management should, in larger organisations, link into established risk management processes and governance arrangements.

8. All organisations must have effective information security event reporting and management procedures in line with Department of Health policies and guidelines.
9. All organisations must ensure that formal contractual arrangements are in place with all contractors and support organisations and that these include compliance with information governance requirements.

Process

10. All organisations must have documented policies and procedures, agreed by the senior management team, to ensure compliance with common law obligations of confidentiality, Data Protection and other relevant legislation in line with Confidentiality: NHS Code of Practice and the NHS Care Record Guarantee or equivalent guidance. Key areas to be covered include, but are not limited to:
 - Consent management and ethical practice;
 - Information sharing protocols;
 - Fair Processing and DPA notification;
 - Subject access request & other DPA requirements;
 - Overseas processing;
 - Confidentiality code of conduct.
11. All organisations must have documented policies and procedures, agreed by the senior management team, to ensure that the information they are responsible for is held securely in line with Information Security: NHS Code of Practice or equivalent guidance. Key areas to be covered include, but are not limited to:
 - Business continuity and disaster recovery;
 - Physical security;
 - Network security;
 - Remote/home/teleworking;
 - Secure data transfer;
 - Access controls and access management;
 - Data and media destruction;
 - Local data warehousing;
 - Cross boundary information sharing.
12. All organisations must have documented policies and procedures, agreed by the senior management team, to establish and implement an effective and comprehensive information lifecycle management framework in line with Records Management: NHS Code of Practice or equivalent guidance. Key areas to be covered include, but are not limited to:
 - Records management;
 - Data flow mapping;

- Records retention;
- Archiving;
- Data quality including NHS Number implementation;
- FOI compliance;
- Environmental Information Regulations ;
- Re-use of Public Sector Information Regulations.

People

13. All organisations must assess training needs annually and ensure that all individuals who contribute to the organisation discharging its responsibilities receive appropriate job/role specific information governance induction and training.
14. Clear and job specific guidance on organisational working practices must be provided to all staff and documented policies and procedures must be easily accessible.
15. All employees of the organisation must have contracts, clearly linked to disciplinary procedures, which require compliance with Information Governance standards. Where practicable, assurances should be sought that similar arrangements apply to other individuals who contribute to the organisation discharging its responsibilities.

Assessment & Audit

16. All organisations must review their compliance with their information governance policies and procedures at regular intervals (at least annually) as determined by the senior management team. External audit/validation must be commissioned for areas assessed as high risk and should be considered for all areas.
17. All organisations must ensure information risk is assessed at regular intervals (at least quarterly) for all major information assets and must take steps to mitigate identified risks.
18. All organisations must review their contractual arrangements annually. Where multiple organisations have similar contracts with the same party, this should be undertaken by a nominated lead organisation that will then disseminate the assurances received.
19. All organisations that provide an annual declaration, such as a Statement of Internal Control or an annual report, must reflect the results of compliance reviews and risk assessments within all such declarations.

ID	Task Name	February		March		April		May		June		July		August		September		October																					
		28	04	11	18	25	03	10	17	24	31	07	14	21	28	05	12	19	26	02	09	16	23	30	07	14	21	28	04	11	18	25	01	08	15	22	29	06	13
38	Develop & Implement IG Assurance Framework	[Gantt bar spanning from 28/02 to 27/07]																																					
39	IG Toolkit v6	[Gantt bar spanning from 28/02 to 27/07]																																					
40	✓ IG Toolkit v6 content agreed with user & stakeholder groups	◇ 31/03																																					
41	✓ IG Toolkit v6 content agreed with NIGB	◇ 23/04																																					
43	✓ DH/ALB toolkit 'views' signed off	◇ 30/04																																					
45	✓ IG Toolkit v6 content sent to Exeter for build	◇ 09/05																																					
47	✓ IG Toolkit v6 Alpha test commences	◇ 02/06																																					
49	✓ IG Toolkit v6 Beta test commences	◇ 16/06																																					
51	✓ IG Toolkit v6 issued for 2008/9 cycle	◇ 30/06																																					
52	Embed in annual reporting processes & procedures	[Gantt bar spanning from 28/02 to 27/07]																																					
53	NHS & ALBs	[Gantt bar spanning from 28/02 to 27/07]																																					
55	NHS Finance Manual updates - consultation ends	◇ 31/07																																					
56	Personal Data Incidents in NHS/ALB annual reports	◇ 20/05																																					
57	✓ IG included in NHS/ALB Statement of Internal Controls	◇ 20/05																																					
58	Foundation Trusts	[Gantt bar spanning from 28/02 to 27/07]																																					
61	Personal Data Incidents in annual reports for 07/08	◇ 16/05																																					
64	Personal Data Incidents in FT annual reports	◇ 30/05																																					
65	IG included in FT Statement of Internal Controls	◇ 30/05																																					
66	Independent Sector	[Gantt bar spanning from 28/02 to 27/07]																																					
67	Ensure NHS std contracts reflect reporting requirements	[Gantt bar spanning from 28/02 to 27/07]																																					
68	Submit to National Standard Contract Board	◇ 23/05																																					
69	Legal review of ISTC contracts complete	◇ 31/07																																					
70	Disciplinary Procedures	[Gantt bar spanning from 28/02 to 27/07]																																					
74	Report & recommendations produced	◇ 31/07																																					
75	New Policies issued to NHS (by NHS Employers)	◇ 01/09																																					
76	New Policies endorsed by Monitor	◇ 01/09																																					
77	Clarification from Professional Regulators	[Gantt bar spanning from 28/02 to 27/07]																																					
78	SUI Enhancement	[Gantt bar spanning from 28/02 to 27/07]																																					
79	SUI Criteria for IG developed	◇ 29/02																																					
80	SUI extended to ALBs	◇ 30/04																																					
81	SUI extended to the Independent Sector	◇ 30/04																																					
82	IG Capacity & Capability	[Gantt bar spanning from 28/02 to 27/07]																																					
83	Online IG Training Tool	[Gantt bar spanning from 28/02 to 27/07]																																					
84	Online IG training tool delivered	◇ 31/03																																					
86	Online IG training tool available for use	◇ 13/05																																					

ID	Task Name	February		March		April		May		June		July		August		September		October																					
		28	04	11	18	25	03	10	17	24	31	07	14	21	28	05	12	19	26	02	09	16	23	30	07	14	21	28	04	11	18	25	01	08	15	22	29	06	13
87	PCT IG Training																																						
88	PCT IG Training Programme approved																																						
89	Supplier appointed																																						
90	Future activity determined																																						
91	UKCGC initiated review of resource requirements																																						
93	Report signed off by UKCGC																																						
94	Report signed off by BMA Managers sub-committee																																						
95	Report published on CFH Website																																						
96	Review of Informatics education & training complete																																						
97	IG integrated into Board level assessment tools																																						
98	Security Standards & Tools																																						
99	Guidance on interim tools issued																																						
100	Central procurement for removable media tools complete																																						
101	GP Back-up tapes																																						
102	GPSOC backup tape encryption solutions commenced																																						
103	Approach defined & requirements issued to suppliers																																						
106	Secure mechanisms for Bulk Data transfer																																						
107	Interim solution defined																																						
108	Interim solution pilot commenced																																						
109	End of pilot evaluation report and future options																																						
110	Fully functional service available for use																																						
111	Enhance Assessment																																						
113	HCC publish Assessment Framework																																						
114	Embed in Standard Operating Frameworks																																						
115	IG Assurance Framework embedded in Operating Frameworks																																						
116	Integration of Governmental & Wider Reviews																																						
117	Overseas data																																						
118	NHS Guidelines published																																						
121	Stakeholders																																						
122	Stakeholder Matrix produced																																						
123	Stakeholder Engagement Plan produced																																						
124	Final Report to Stakeholders																																						

Appendix 4 – Risk and Issues Log

The programme risk & issue log is replicated below as at the end of June 2006. There is an additional column to show whether each risk or issue is closed, or if it remains open, where ownership is transferred.

ID	Risk or Issue	Title	Description	Impact	Probability	Controlability	Action Plan	Progress against plan	Status at closedown
1	Risk	A relevant organisation is omitted from the scope of the Programme	The programme needs to address all organisations within the scope of DH and the NHS. Critically it is all organisations that, should an issue occur, the media and public would regard as being part of the DH/NHS and/or accountable to the Secretary of State for Health.	Failure to address IG issues in all relevant organisations	High	B	<ol style="list-style-type: none"> 1. Create an initial list of organisations 2. Distribute the list for wide review 3. Compare the list with other available sources of information 4. Establish activities and plans to ensure that organisations' responsibilities are articulated in a single place (particularly PCTs). 	<ol style="list-style-type: none"> 1. Initial list attached as an Appendix to the PID 2. 8 week piece of work initiated by Tony Long to define the organisations and their lines of accountability, due to complete 9/5/08 3. The list of Organisations in scope has now been established and is being checked to ensure all organisations have been included. 	This is an ongoing risk for the furtherance of IG within the whole enterprise. There is an organisation mapping activity that will also include lines of accountability and there are recommendations regarding this as this will need to be owned and maintained going forwards. This risk is owned by the DH SIRO following Programme Closure.

ID	Risk or Issue	Title	Description	Impact	Probability	Controlability	Action Plan	Progress against plan	Status at closedown
2	Risk	Assurances from Foundation Trusts may not be adequate	Due to their status, assurances from Foundation Trusts may be inadequate or absent	There will continue to be breaches of confidentiality/ data loss	High	B	<ol style="list-style-type: none"> 1. Negotiations with Monitor 2. Engage with the Foundation Trust Network 3. Establish relationship for ongoing dialogue 4. understand how Monitor performance manages FTs 	1. Monitor actively engaged and progressing with FTs	This risk is owned by Digital Information Policy following programme closure
3	Risk	Assurances from independent contractors (e.g. GPs) may not be adequate	Assurances from independent contractors may be inadequate or absent	There will continue to be breaches of confidentiality/ data loss	High	C	<ol style="list-style-type: none"> 1. Apply pressure through relevant groups (Royal Colleges, GMC etc) 2. Provide incentives/training (e.g. IM&T DES) 3. Long term – embed in contractual arrangements 4. Use audit capability under SOC 5. Opportunities to be investigated to put appropriate linkages into GP Contracts. 6. BAU activities to cover pharmacies, dentists and opticians. 	<ol style="list-style-type: none"> 1. DIP are leading work to engage the GP community. 2. Good progress is being made with the Royal Colleges. 3. Changes to the GP Contract are complex and political and subject to protracted negotiations each year. This remains a long-term goal. 	This risk is owned by Digital Information Policy following programme closure

ID	Risk or Issue	Title	Description	Impact	Probability	Controlability	Action Plan	Progress against plan	Status at closedown
4	Risk	Organisations fail to meet the required standards	Organisations may fail to meet the standards developed by the programme in the time required	Inadequate standards of IG in some organisations	Medium	C	<ol style="list-style-type: none"> 1. Engage with all organisations as soon as possible to ensure that they are aware of current & emerging standards 2. Maintain communication throughout the programme 3. Involve representatives from the field to ensure that standards developed are realistic and achievable 4. Audit Commission's ALE (Auditors Local Evaluation) to be appropriately amended. 	<ol style="list-style-type: none"> 1. Tasks added to plan for: Disciplinary procedures; work with Healthcare Commission; Improving capability & capacity. 2. Regular communications established 3. workshop on 7/5/08 to determine the exact nature of the IG Assurance Framework going forward 4. Discussions have been held with the Audit Commission to ensure that their materials have appropriate content. 	This risk can be closed. Business as usual activities across a number of groups address this.

ID	Risk or Issue	Title	Description	Impact	Probability	Controlability	Action Plan	Progress against plan	Status at closedown
8	Risk	Insufficient Resources to address all issues	There is no new money for IG. Existing resources (human and financial) may be insufficient within some or all organisations	Organisations may need to divert resources from elsewhere, or fail to meet the required standard	High	C	<ol style="list-style-type: none"> 1. Highlight the risk to all organisations 2. Investigate procurement routes for resources (Action PB 03/02) 3. Further details of the procurement routes available are to be published in the next IGAP Update. 	<ol style="list-style-type: none"> 1. CFH informed 2. SHA CIOs informed. 3. Procurement routes for resources have been investigated and the only national route is the OGC framework. 	This risk is owned by the DH CIO as the head of Information Governance across the DH, its Arms Length Bodies and the NHS.

Appendix 5 – Summary of Recommendations

The following table lists all the recommendations from the main body of the document, along with the owner and timescale for taking the recommendation forward following programme closure.

No	Recommendation	Owner	By When
1	Any organisation which hosts another body within it must treat that body as part of its own organisation for the purposes of information governance.	CIO for Health	Immediate ⁴
2	The list of organisations and lines of accountability of all such non-statutory bodies should be owned and maintained centrally within the Department of Health as a valuable resource for managing its business.	DH Finance Director	Immediate
3	Complete discussions with the Audit Commission regarding further NHS Audit activity, including any resource implications.	DH Director of Performance	31/12/08
4	Work should be undertaken to formally bring independent contractors into the IG Assurance Framework as soon as is practicable.	Head of DH Digital Information Policy	A Plan to achieve this to be agreed by 31/03/09
5	Options for changes to the GMS contract should be considered at the earliest available opportunity.	Head of DH Digital Information Policy	31/03/09
6	Work should be undertaken to formally bring all ALBs into the IG Assurance Framework by 01/04/09.	Head of the DH ALB Business Support Unit	31/03/09
7	The NHS Manual of Accounts for 08/09 and thereafter and its associated guidance should be amended to reflect IG requirements.	Head of the NHS CFH Access Controls Team	31/12/08
8	IG Education Training & Development should be further developed to reflect the requirements of the NHS and other users.	Head of DH Digital Information Policy	A 2 year programme to be established by 30/09/08

⁴ Subject to the date of the new CIO for Health taking up their appointment

No	Recommendation	Owner	By When
9	Two new national groups should be established: a National IG ETD Reference Group; and a National IG ETD User Group.	Head of DH Digital Information Policy	30/09/08
10	The work required to embed Information Governance within the Integrated Governance Handbook should be concluded.	Head of the NHS CFH Access Controls Team	31/12/08
11	Further work should be undertaken to ensure that IG is referenced appropriately in guidance for Boards.	Head of DH Digital Information Policy	31/03/09
12	Further work should be undertaken to develop guidance on overseas Processing of Personal Data.	Head of DH Digital Information Policy	31/12/08
13	Further work should be undertaken to ensure that the Healthcare Commission's assessment criteria appropriately reflect IG requirements.	Head of DH Digital Information Policy	30/09/08
14	Further work should be undertaken to develop and consult on guidelines for effectively resourcing IG for different organisation types	Head of DH Digital Information Policy	31/12/08
15	Further work is undertaken to ensure that a nationally available solution to the secure transfer of bulk data is available for use by 31 st December 2008.	Head of the NHS CFH Infrastructure Security Team	31/12/08
16	Independent sector providers of NHS services should be permitted to assume responsibility for the management of access controls for their staff needing to access NHS CRS applications by establishing Registration Authorities according to strict criteria.	Head of the NHS CFH Access Controls Team	31/12/08
17	Further work is undertaken to complete the review of confidentiality and disciplinary procedures	Head of the NHS CFH Access Controls Team	30/09/08
18	Further work is undertaken to ensure that the ALBs have a consistent approach in their organisations regarding confidentiality and disciplinary policies.	Head of the DH ALB Business Support Unit	31/12/08

No	Recommendation	Owner	By When
19	Further work is undertaken to inform the Cabinet Office and Ministers about the approach proposed for meeting the Cabinet Office requirements in the NHS and to seek Ministerial agreement where there are issues of practicality and/or resources.	Head of DH Digital Information Policy	30/09/08
20	Further work is undertaken to ensure that both the central IS Contracts (by April 2009) and the Standard NHS contracts (by October 2008) include appropriate reference to the requirements of the Information Governance Assurance Framework	DH Director of Performance	31/03/09
21	On behalf of the acting CIO for Health, the IGAP executive team (renamed as the IG Executive) should continue to meet on a fortnightly basis, in order to complete any residual actions and transfer to business as usual activity, chaired by Philip Brown with support from DIP. This to be reviewed at the end of October.	Head of the NHS CFH Access Controls Team	Immediate
22	The Information Governance Assurance Framework to be promoted as the collective brand name for all the components identified in section 8.1	Chair of the IG Executive	A Plan to achieve this to be agreed by 31/10/08
23	The CIO for Health should be the owner of the Information Governance Assurance Framework.	CIO for Health	Immediate ⁵
24	The NIGB should oversee and report on the findings of an annual review of the national components of the Information Governance Assurance Framework and organisations' compliance.	CIO for Health	First annual review to be undertaken during Q1 2009/10 ⁵
25	All organisations delivering or supporting delivery of NHS services should be required to meet the Information Governance Standard and provide assurance through completion of an annual performance assessment through the Information Governance Toolkit.	CIO for Health	31/03/10 ⁵

⁵ Subject to the date of the new CIO for Health taking up their appointment

No	Recommendation	Owner	By When
26	Develop options for Ministers in respect of the mandation of specific levels of performance against key requirements in the information governance toolkit, including proposals for consultation on implementation timescales where appropriate.	Head of DH Digital Information Policy	30/09/08
27	The CIO for Health is accountable to the Permanent Secretary and the NHS CEO for the delivery and maintenance of the Information Governance Assurance Framework.	CIO for Health	Immediate ⁶
28	The CIO for Health should identify a member of his/her management team to provide leadership for IG in the DH and those bodies it hosts in IG terms (e.g. those ALBs which are not corporate entities).	CIO for Health	30/09/08 ⁶
29	A Department wide Information Governance Steering Group should be established chaired by a senior manager with responsibility for IG.	CIO for Health	30/09/08 ⁶
30	The DH establishes a single Information Asset Register covering the information assets in all its constituent bodies.	CIO for Health	30/09/08 ⁶
31	The DH allocates Information Asset Owners for each of the Information Assets at a Director level.	CIO for Health	30/09/08 ⁶
32	The DH establishes an appropriately resourced Caldicott function and clearly defines roles, support arrangements and delegated authority.	CIO for Health	30/09/08 ⁶
33	The DH should clarify and document the relationships between the information risk management, information governance and Caldicott functions.	CIO for Health	30/09/08 ⁶
34	Ministerial reporting in respect of data losses within the NHS and Independent Sector should be undertaken by the NHS Business Unit	DH Director of Performance	Immediate

⁶ Subject to the date of the new CIO for Health taking up their appointment

No	Recommendation	Owner	By When
35	Establish a reporting mechanism for the DH and its entire delivery chain that aligns with the Cabinet Office and the Information Commissioner’s requirements and public expectations.	DH Director of Performance	31/12/08
36	Strong working relationships should be developed to ensure that relationships with external bodies are managed consistently and effectively.	CIO for Health	31/12/08