The National Archives

Information Management Assessment

Department of Health

Reviewed

October 2014

Published

May 2015

Working with government **to raise standards in information management**

Contents

Statement of commitment

The following statement was provided by the Permanent Under-Secretary of the Department of Health. It was published as a component of a news story on the department's intranet site in September 2014

> The Department of Health is committed to making sure that it manages, protects and exploits the information it holds and works with as part of its corporate obligations.
>
> To show the strength of the department's commitment I have asked the National Archives to review our processes and systems. The National Archives regularly conducts assessments of Information Management practices and compliance within government departments. The report they produce will help me to support all aspects of Knowledge and Information Management across the department so that our information is appropriately captured, managed and preserved, and information risks and sensitivities are appropriately handled.
>
> Una O'Brien
> Permanent Secretary

IMA background

The Information Management Assessment (IMA) entailed a detailed review of supporting documentation followed by interviews with senior staff, specialists and practitioners in the department's London and Leeds Offices. These were conducted between 13 and 24 October 2014. Additional interviews with key staff were conducted in person and by telephone into November.

The following report provides a summary of good practice as well as risks identified in the course of the assessment. IMA reports and departmental action plans are published on The National Archives website and can be accessed at: http://www.nationalarchives.gov.uk/information-management/our-services/ima-reports-action-plans.htm

Key findings of the assessment

1 The value of information

Performance rating	
Communicating and realising value	**Satisfactory**
Managing information as an asset	**Development area**

- The Department of Health policy for information management communicates to staff five key principles for the effective protection, management and exploitation of information (see p. 15). It clearly conveys the importance of information to the organisation. This message is supported through explicit links made to the department's business strategy and in the personal endorsement provided by the Permanent Under-Secretary. Consistent messages are also set out in the department's information assurance policy.
- The current ICT strategy 2013–15 has an information management component, which focuses on the roll-out of the department's SharePoint system, Information Workspace (IWS). The department has also produced a draft IWS strategy, which is principally directed towards the development of this system and related tools. Although the strategy has not yet been adopted, its development shows a clear determination to improve and embed IWS as an enabling tool for the business. Plans to increase stability, deliver records management outcomes and better meet user needs should be prioritised and supported. At the same time, this report emphasises that the department needs to provide proportionate direction for the technology environment as a whole, including the shared drives and the information held within them. It should give due consideration to culture and governance alongside technical considerations. The former should include encouraging compliance with corporate policy and embedding good practice within business process. In implementing its strategy for 2015 onwards, the department would benefit from adopting its own five principles for information as an overall focus.

- The department requires its Divisional Heads, as Information Asset Owners (IAOs), to record any significant information assets on the Information Asset Register (IAR) and conduct risk assessments on them. However, the department currently does not provide its IAOs with a single definition of an information asset or clearly expressed criteria to support their identification. The department should address this to support a uniform and consistent approach to managing, protecting and exploiting its information assets. It needs to consider how greater coverage can be given to the broad groupings of unstructured information within key corporate repositories such as IWS and the shared drives. The department has made a start in bringing unstructured information within the scope of its information asset governance approach by describing how IAOs should be supported by the custodian role. The department should build on and formalise these requirements to help leverage good practice in information and records management. The department's information asset register records only a basic level of context and should be expanded and developed.

2 Digital information and supporting technology

Performance rating	
Supporting information through technology	**Development area**
Digital continuity and IT change	**Development area**

- In principle, IWS can provide a supportive environment for information and records management. However, the department's shared drives hold more information and are growing more rapidly than IWS. These are not subject to central oversight or control and do not support disposal. Records are not yet routinely being declared and disposal has not yet been enabled within the main shared resources area of IWS where records of short, medium and long-term value should be stored. There are also indications that email inbox limits are driving staff to delete emails in bulk or transfer them in bulk to IWS without considering their value. The department is

considering the introduction of an email archive to address this. If it does this, it must assess and monitor the impact on records creation.

- The department has no formal digital continuity plan and lacks understanding of the digital information it holds across all repositories. Once it has clarified its definition of an information asset, it should seek to identity at a proportionate level what information assets are held and who owns them. The department has responsibility for 19 million digital records inherited from Primary Care Trusts (PCTs) and Strategic Health Authorities (SHAs) and also holds legacy records within the Lotus Notes based MEDS system. It is strongly recommended that the department develops a plan to support the long-term completeness, availability and usability of information within these repositories and the shared drives.

3 Information risk, governance and oversight

Performance rating	
Recognising information risk	**Development area**
Establishing control	**Satisfactory**
Providing guidance	**Development area**
Measuring impact	**Good practice**

- The assessment team noted a number of positive approaches in relation to information risk. For example, the team was pleased to note that the Health Group Internal Audit function subjected to scrutiny the 2012 relocation of the department's filestore from former premises. The team also recognises that the information risk assessment process for information assets identified by the business allows a range of information risks to be raised. However, in overall terms, the department has not yet fully defined the potential impact of information and records related risk. Its overall approach to information risk prioritises information security with a focus on the potential loss of personal data. In parallel to this, it should also formally articulate the risk at all levels of a failure to capture or keep

the information it needs, in line with its value. The Senior Information Risk Owner (SIRO) must be sighted on this risk and the department needs to know in what ways, and how successfully, it is being mitigated.

- In terms of overall governance, the department would benefit from reviewing current provision of information-focused boards to ensure long-term planning is supported as well as oversight at an operational level. The department has an established network of Local Folder Managers (LFMs) who have a key role to play in ensuring the effective operation of IWS. The department is currently working hard to engage and support the network through regular meetings and communications. To help ensure that full benefit is achieved from the LFMs, the department should make the draft LFM performance objective mandatory and build it into the performance evaluation framework. It should also define how LFMs support IAOs, and seek assurance from IAOs that necessary arrangements are in place, as part of the work to formalise the relationship between IAOs and custodians recommended by this report.
- The department's Information Management Policy was conceived as a single document, but has lost impact now it has been divided into a series of web pages. It needs to be reviewed to ensure principles are promoted to best effect. The department has produced a retention schedule and provides staff with a definition of a record. However, it also needs to provide proportionate 'What to Keep' guidance to help staff recognise the value of information and how it needs to be handled. A lack of clarity in this regard may have played a part in the bulk saving of emails. The department must ensure that all staff who use IWS receive the training they need.
- The department's internal programme of assessments provides a helpful means of measuring compliance with information management policy and of encouraging good practice. Individual assessments have a wide scope and considerable effort has been invested in maintaining the programme. The department should ensure that results are more widely publicised so that directors in their capacity as IAOs can see how their teams are performing. It should continue to build on the good start that has made

with the internal assessment programme, with a view to delivering more in-depth and qualitative assessments of standards of information management within IWS and the shared drives.

4 Records, review and transfer

Performance rating	
Oversight of records and selection	**Satisfactory**
Implementing disposal decisions	**Satisfactory**

- The department has a good track record in the appraisal, preparation and transfer of paper records. Although not due to transfer digital records until 2020, it should begin now to develop plans for their appraisal. In addition to the 19 million digital records inherited from PCTs and SHAs, the department also inherited almost 475,000 boxes of paper records. These are managed alongside the department's own records under the NHS Code of Practice and are unlikely to be transferred to The National Archives. However, they will still need to be reviewed and should be factored into the department's plans for records in all formats in view of their potential impact on its continued ability to meet the transition timeline for the 20-Year Rule.
- Records are being disposed of from MEDS. However, as highlighted above, disposal is not enabled within the shared drives or shared resources area of IWS. The department needs to enable disposal within IWS and define how it will be applied to information currently held within its shared drives. It also needs to work with The National Archives to identify a suitable solution for the sensitivity review of digital records.

Highlights table

The following are among the areas of good practice at the time of the assessment specifically highlighted in this report. These highlights include systems and approaches that other government organisations may find helpful in mitigating information and records management related risks.

Policy for information management sets expectations in terms of how information should be protected and exploited as well as how it should be managed. The policy sets out the benefits of good practice for the business and is personally endorsed by the Permanent Under-Secretary. It establishes five principles for staff that are also highlighted in information assurance policy.
The department actively sought to learn lessons following the replacement of its Electronic Documents and Records Management System (EDRMS) with SharePoint-based Information Workspace (IWS). A customer insight survey helped to identify common issues and concerns in relation to the new system, which have been used to inform a draft IWS strategy and action plan.
Departmental guidance on information risk highlights the benefits of transparency and underlines the risk of not sharing information in addition to the risk of losing personal and sensitive data.
The department has worked actively to establish a centrally-supported network of Local Folder Managers (LFMs) to help enable the effective administration of IWS. Regular meetings and newsletters are used to deliver key messages, promoting quick wins and helpful case studies, and conveying key future changes.
The department has published its retention and destruction policy publicly on GOV.UK
The department has established an internal programme of assessments and positioned this as the means by which compliance with information management policy will be understood and monitored. Assessments are targeted towards the five principles that the information management policy establishes for staff.

The department has worked to define trigger dates within folders in IWS to activate disposal.
The department has run a ‘Secure Information’ campaign about information security, with the endorsement of the Permanent Under-Secretary. The core messages of the campaign were delivered through a variety of channels including video clips on the intranet and hosted on the department’s YouTube channel, along with postcards and posters. In parallel with this campaign, compliance checks were carried out on the department’s clear desk policy.

Recommendations to address risk areas

Recommendation 1
Ensure that information strategy and vision for 2015 onwards is signed off at Board level with an agreed schedule for reporting so that progress in delivering benefits can be monitored and challenged. ***Priority should be given to improving and embedding Information Workspace (IWS) and enabling routine records creation and disposal. The strategy must provide impetus for effective lifecycle management, protection and exploitation of information across all repositories.***
Key supporting requirements include: • Alignment with the department's five principles of information management and current business priorities. • Defining information and records management outcomes for the technology environment as a whole, as the department works to stabilise IWS and better align it to user needs. This must include a greater focus on the shared drives and the information they contain. • Giving attention to the role of culture and governance in driving the appropriate use of systems alongside technical considerations. • Creation of an information board with a strategic focus to facilitate long-term planning.

Recommendation 2
Review how information assets are defined and logged, and how owners are allocated. This should be done with a view to increasing understanding of the information for which the department has responsibility and helping to better manage, protect and exploit it.
Key supporting requirements include: • Adopting a single definition of an information asset and defining how information asset governance and information and records management are linked and support each other. • Clarify how the definition of an information asset should be applied, including to broad groupings of unstructured information held in key corporate repositories such as IWS and the shared drives. • In line with this, formalising requirements for information custodians and

establishing parameters for provision of assurance by IAOs that necessary steps have been taken.
- Providing a clear line in policy on the roles that support IAOs in the provision of assurance and how they work together.
- Expanding the Information Asset Register (IAR) to document a wider range of context about information assets such as value, purpose and disposal requirements.
- Engaging with the IAO training programme delivered by The National Archives.

Recommendation 3

Refresh and raise the profile of guidance to staff on how systems need to be used. Encouraging adherence to core principles should be a key component of the department's overall strategic approach for its information.

Key elements that should be prioritised include:

- Reviewing how information management policy is published to ensure key requirements and mandate are being promoted to best effect.
- Clear policy statements and guidance on the role that the shared drives fulfil in relation to IWS and as a repository for records. These should be updated as the department's overall strategy for IWS and the shared drives is implemented.
- Clear guidance to staff on what information needs to be saved into team and shared resource areas in IWS.
- Clear guidance to staff on how, why and when to 'check in' and 'declare' records, while continuing to investigate technical solutions that may reduce the burden in this regard.
- Clear guidance on how disposal operates and what benefits it offers to teams, individuals and the department as a whole.
- Ensuring that all staff who need to use IWS receive training.

If the department introduces an email archive with automated disposal it must also ensure that staff understand the continued need to capture information with value within corporate systems. It should also monitor the impact on records creation.

Recommendation 4

In line with information management policy, support the KIM team and Local Folder Manager (LFM) network to push back where requests to restrict access to information are judged unnecessary

This would be supported by:

- Devising an escalation route to senior stakeholders if and when pressure is applied.

Recommendation 5

In alignment with the department's overall strategic approach, devise a long-term plan for ensuring digital information is complete, usable and available as long as needed. This should focus on MEDS, the shared drives and Primary Care Trust (PCT) and (SHA) records.

This would be supported by:

- Running a tool such as DROID (The National Archives' free tool for Digital Record Object Identification) over key repositories to understand the age and format of information.
- Defining clear parameters for information within the shared drives, including migration of information, disposal of information and decommissioning of the drives
- Considering the future migration of information in MEDS to a more sustainable system.
- Ensuring that metadata supports the retention, scheduling and management of records and their transfer to The National Archives.

Recommendation 6

Support the Senior Information Risk Owner (SIRO) by defining and communicating the risk of not capturing or keeping information in accordance with its value so that it can be addressed at all levels of the department. This should encompass cultural, governance and technology-related causes and business- and compliance-related impacts.

This should be supported by:

- Establishing the position of the Departmental Records Officer (DRO) and other information management, security and assurance roles within information governance accountabilities. This is important to clarify their role in relation to the SIRO.
- Reviewing mitigating factors currently defined for the risk of loss of sensitive or personal data. These should emphasise actions carried out by IAOs, not the appointment of IAOs.

- Explicit reference to information and records management in the headline statement of principles for new information assurance policy.

Recommendation 7

Produce a plan to ensure continued support for the LFM network as a key means of enabling effective management of information through the term of the information strategy.

This should be supported by:

- Embedding the LFM performance objective within the performance management framework and defining how LFMs help mitigate information and records management related risk.
- Setting clear expectations for the business in terms of continuity of the role and ensuring it is supported.

Recommendation 8

Establish the scope of the department's own internal IMA programme for the term of the information strategy so that it can continue to help drive good practice and monitor compliance.

This should be supported by:

- Ensuring that internal assessments cover records creation and declaration, how well 'What to Keep' principles are being applied by teams, and how well shared drives and IWS are being used.
- Publishing results from internal assessments more widely so that IAOs can see how successfully policy is being adhered to.
- Testing compliance with requirements for information custodians once formally established.
- Closer alignment of the Information Risk Assessment and internal IMA process.

Recommendation 9

Produce and promote guidance for staff to help them understand in practice what information has value and how it needs to be managed as a consequence. Promotion of principles should be a key component of the department's overall strategic approach for its information.

This would be supported by:

- A clear statement on who needs to capture information (including email) and when this needs to be done.
- Incorporating 'What to Keep' within the scheduled 'Storing Information' campaign or making it the focus of a subsequent campaign.
- Ensuring that 'What to Keep' guidance is the basis for any decisions to review and delete information from the shared drives.
- Ensuring that the DRO's responsibilities are extended to encompass the shared drives and disposal of information assets.

Recommendation 10

Devise a plan and approach for the appraisal, selection and sensitivity review of digital information.

This would be enabled by:

- Drawing on The National Archives' advice and guidance.
- Ensuring the plan covers all digital information in all repositories.

Recommendation 11

Ensure that PCT and SHA records are bought within wider plans for the management of records in all formats.

This must be accompanied by:

- Clear planning for the management of these records that factors in agreed and available resources.

1 The value of information

1.1 Communicating and realising value

IMA goal: The organisation establishes information's value in principle and supports its realisation in practice.

Establishing the importance of information

The Department of Health Information Management Policy was signed off in June 2014. The policy reflects many of the key requirements of the Section 46 Code of Practice and it is personally endorsed by the department's Permanent Under-Secretary, Una O'Brien.[1] In her foreword, she states that adoption of the policy will support achievement of the department's key objective of public accountability, enable greater effectiveness and efficiency, and underpin efforts to transform the department. Further highlighted benefits within the policy include improved ability to deliver transparency and open data goals. It establishes the department's commitment to good practice in information and records management as a central component of business strategy. It also establishes the responsibility that staff have, both for managing information and for preserving, protecting and sharing it. **This is good practice.**

The policy sets out the following five principles as minimum requirements for staff:

- obtain and use information legally and fairly
- organise information so that it is accessible, can be located easily and is available for re-use by others
- store and transfer information securely
- share and publish information appropriately
- proactively manage information through to its destruction.

[1] http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf

Specific responsibilities are defined for managers. These include the promotion of 'Responsible for Information' training and the creation of an environment where 'information management is seen as a priority and an integral part of routine work rather than as an additional burden'. The accompanying Retention and Destruction policy states that information held by the Department 'needs to be managed like any other asset'. It states 'all information that is useful to the business is part of our corporate memory which helps us discharge our responsibilities for public accountability, and it needs to be retained for as long as it has value and destroyed as soon as possible afterwards.' **This is good practice.**

The department's information assurance policy and strategy also provides a number of linked and supporting statements and highlights the above five principles. This establishes a vision of information as a critical business asset that needs to be protected and shared carefully 'where this will benefit individual patients and improve standards'. The document highlights the 'timely secure disposal of information in line with our records management policy' as one of the means by which information assurance is achieved. This document was under review at the time of the IMA. The department should use this opportunity to fully embed the role of information management and explicitly refer to it in the new information assurance policy's headline statement of principles. **See Recommendation 6.**

Setting goals and championing information and its management

The Department of Health ICT Strategy 2013–15 is intended to drive:

> 'the implementation of better management processes, strengthen our capability and better policy making through the digital tools, technologies and services that are available'.

The strategy is high-level, does not include or reference a more detailed implementation plan or reporting requirements, and is not formally endorsed or signed off. Positively, however, it is aligned with information management as well as IT-related outcomes. This is one of its four areas of focus alongside

open service ICT delivery, the transformation of business systems and the enabling of mobile and flexible working.

The information management strand is centred on the delivery of an integrated document and records management solution through Phase One of the department's Enterprise Content Management (ECM) Programme. This took place in Spring 2013, when the department replaced its in-house developed, Lotus Notes-based, Electronic Documents and Records Management System (EDRMS), MEDS, was replaced. This system had been in place since 2004.

The selection of the replacement and its rollout was tied to a wider desktop systems upgrade. The department was channelled towards a SharePoint 2010 based solution, Information Workspace (IWS), using the Automated Intelligence Compliance Extender and SyncPoint to extend records management capability and enable connection with Microsoft Outlook. The link to a wider IT overhaul also meant that rollout of the system had to be completed within 10 months. This left limited time for business engagement or training. At the time of assessment, some 3,400 staff had access to the IWS, but take up of the system was still reportedly low and the department's shared drives were still in active use.

A lack of technical knowledge and expertise in relation to SharePoint is understood to have impacted the implementation of IWS. The new system experienced a period of severe technical failures from December 2013 to March 2014, which had a significant impact on performance. The assessment team understand that this was largely due to issues with SyncPoint and email synchronisation. During this time IWS was extremely slow and on occasion staff were unable to access the system and information held within it. The considerable impact that this had in business terms was underlined by a number of interviewees. Other problems encountered included the apparent disappearance of documents that staff believed had been saved to the system.

The assessment team recognises that the department has taken steps to address the IWS's performance issues and a number of interviewees expressed confidence that the system had now 'turned a corner' in terms of its stability and usability. However, initial challenges experienced during implementation have had an impact on users' faith in IWS, and a significant number of interviewees expressed strong negative views in relation to the system. The assessment team also saw indications of a lack of clarity on the department's expectations in terms of information management although IWS is established in current information management policy as the 'preferred place for managing documents'. One senior manager, who described IWS as a tool to ease the email burden rather than a records management system, asked members of the assessment team if they knew 'where we should be storing records now MEDS has gone'. Another commented, 'I no longer know how you are meant to file or search – can the department tell me what the means of overcoming the current problem is'.

The current ICT strategy 2013-15 is now coming to an end. In recognition of the difficulties surrounding the introduction of IWS, the department carried out a customer insight survey to identify common issues and concerns. Survey results have informed a draft IWS strategy and action plan, which aims to improve user experience, regain trust and increase use of IWS. The draft document includes insights and lessons learned from IWS design, development and roll out, conveys user views and current risks, and sets out recommendations and proposed activities under an overarching, phased SharePoint Programme. This is a **proactive, good-practice approach**.

However, the assessment team notes that the draft IWS strategy was not signed off at the time of the IMA and existed in isolation without links to the IT strategy. The department has no separate overarching information strategy and both the IWS strategy and the information management component of the IT strategy are focused on IWS and not other systems where information is stored.

While IWS is deserving of continued attention and focus, it must be positioned in a wider strategic context. It must be recognised as one means by which outcomes for the effective management, protection and exploitation of information may be promoted rather than positioned as an end in itself. To support this, the department needs to define required outcomes for its information and then work at a strategic level to ensure that systems, culture and governance together will enable their achievement. It needs to ensure both that IWS supports staff and that staff are encouraged to use it correctly. It must also encourage good practice across all repositories, including the shared drives where a considerable volume of the department's information is held. To facilitate a joined-up approach, the department should direct its strategy and vision towards both current business priorities and the five information management principles referenced above.

To provide necessary momentum and establish its priority, the department's approach should be endorsed and signed off at a senior level. This may most appropriately be provided by the Senior Information Risk Owner (SIRO), given the role's responsibility for managing information risk from a strategic and business point of view and in championing an effective information culture. **See Recommendation 1.**

Enabling public access to information and supporting transparency and re-use

Latest figures at the time of assessment showed that the department answered 100% of requests under the Freedom of Information (FOI) Act 'within time' in all but two quarters since 2012.[2] Interviewees indicated that established strong performance in terms of FOI encouraged engagement when requests were received or chased. Internal processes described to the assessment team appeared robust, with weekly meetings held by the FOI team to track the progress of requests and identify any issues that need addressing or escalating.

[2] https://www.gov.uk/government/statistics/freedom-of-information-statistics-july-to-september-2014

As at December 2014, there were 2,515 publications by the department on GOV.UK, 96 of which were classed as transparency data. The department has published 224 datasets on data.gov.uk. This report also notes that the values and behaviours work stream of the 'Our DH' programme references the importance of driving a culture of openness and transparency. **This is good practice.**

1.2 Managing information as a valued asset

IMA goal: The organisation protects, manages and exploits its information assets to achieve maximum value.

Defining and cataloguing information assets

The department provides its Information Asset Owners (IAOs) with a risk assessment template which must be completed for each of their information assets. IAOs are also required to ensure their information assets are recorded on an Information Asset Register (IAR). While a range of context about an information asset may be identified within an individual risk assessment, the IAR itself allows only a basic and limited level of context and detail to be documented. It provides columns to log an information asset's name, the name of the IAO and the staff that support them in the provision of assurance, the responsible directorate and to indicate whether the information asset contains personal data. Information assets containing particularly sensitive data requiring additional risk assessments, such as abortion notifications, are highlighted in bold. While the inclusion of this context is positive in itself, the IAR makes no provision to record what an information asset is and how it is used, the value that the business has identified, disposal requirements, key threats that need to be mitigated or key opportunities that should to be exploited. The department could be doing more to use its IAR as a management tool and should expand it to capture a wider range of context about its information assets. **See Recommendation 2.**

The department currently defines an information asset in a number of different ways. Descriptions within information policy and information assurance policy and strategy indicate that an information asset is a collection of information with recognised value to the business and actively managed content. The Information Asset Owner (IAO) Information Risk Assessment template does not reference actively managed content, but indicates that information systems with value to the department, as well as collections of information, can be defined as information assets. Newly produced guidance titled 'Managing information risk: your responsibilities' establishes sensitivity as a criteria for deciding whether an information asset should appear on the information asset register (IAR), but states that 'information assets are bodies of information such as databases, paper and electronic files, collections of statistics and research findings'.

To enable a consistent approach to information asset governance, the department needs to provide and promote a single definition of an information asset. Because the department places the onus on the business to identify information assets, it must ensure that staff can apply clear and uniform criteria for their identification. **See Recommendation 2.**

As a component of this, the department should establish more clearly how information asset governance and information and records management are linked and how they support each other. Particular consideration should be given to bringing unstructured information held in key corporate repositories within scope of the department's information asset governance regime in a meaningful and proportionate manner. Currently, the department has adopted a high-level and inconsistent approach by defining IWS and MEDS as information assets on its IAR, but not the collaborative platform DHeXchange, or the shared drives, where a high volume of the department's information is held. In addition, while the department's current system-focused approach is useful for highlighting the limitations of these systems and identifying whether controls are operating properly, it can only provide limited insight into how the broad groupings and collections of information they contain are being managed, protected and exploited. To achieve greater understanding and

gain effective assurance that necessary standards are being met, the department needs to focus its approach at a more granular level. **See Recommendation 2.**

Allocating owners

The assessment team saw varied understanding of the IAO role. For example, while one senior manager told the assessment team of recent discussion in their area about whether a particular dataset should be categorised as an information asset, others appeared unaware of both the IAO and SIRO roles. Similarly, one interviewee provided a clear definition of the role of an IAO as 'ensuring the security and integrity of data, preventing its corruption, ensuring it gets to the right people and that personal data is protected and not exposed unnecessarily'. The interviewee was, however, unaware who their IAO was or whether their own business area held any information assets.

IAOs are appointed at director level. Staff interviewed indicated that the seniority of the IAO role means that responsibilities are necessarily delegated in practice. However, while the IAR lists an information asset manager and information asset coordinator next to each information asset, the assessment team found a lack of clarity about their responsibilities. There is also no mention of these roles in information assurance policy and strategy or in information management policy. It is vital that IAOs are supported to provide effective assurance. This report recommends that the department reviews current arrangements. **See Recommendation 2.**

Although information management policy does not reference either information asset managers or coordinators, it does describe the relationship between IAOs and custodians. These include Local Folder Managers (LFMs) appointed to take care of and help manage information in IWS. The policy states that IAOs should ensure information is managed through its lifecycle, stating that IAOs should enable this by ensuring:

- administrators are appointed to manage access to records held in IWS or other systems that hold records
- teams manage shared drives, mailboxes and IWS team areas
- those delegated to manage information have contact details published and maintained.

These steps would provide a potentially helpful basis for supporting good practice in information and records management within IWS, the shared drives and other corporate repositories. To help solidify the links between information asset governance and records management (as recommended above), this report recommends that the department formalises requirements in relation to information custodians and requires the provision of assurance from IAOs that necessary arrangements are in place and working. Compliance may be tested through the department's own internal assessment process (see below, pp. 45–6). **See Recommendations 2 and 8.**

2 Information and supporting technology

2.1 The technology environment

IMA goal: The technology environment supports the management, protection and exploitation of information.

Corporate storage of information

The department's original EDRMS, MEDS, is now closed to new records, making it a legacy system. The draft IWS strategy describes the records management function offered by its replacement, IWS, as 'adequate but basic'.

IWS is divided into two broad filing areas: a team area and a shared resources area. Retention periods of 3, 8, and 15 years have been applied within the shared resources area, which is intended to be for records of corporate value. The team area is for information only of use to the team itself. Interviewees expressed some confusion over what information should be stored in these areas, and records of corporate value are potentially being saved into the team area by mistake. Disposal has not yet been switched on for the shared resource area. However, as team areas are set up to support the automatic disposal of information after two years, there is a current risk that information of corporate value wrongly stored here will be lost to the organisation. To support the effective operation of IWS, the department needs to ensure that staff understand what information needs to be saved into each area. **See Recommendations 1 and 3.**

In practical terms, staff can create documents within the new system and the process of saving information into IWS is fairly simple (particularly with email). From a technical point of view, IWS provides the department with the capability to manage digital information throughout its lifecycle, including creating filing structures, capturing metadata, enabling search, controlling access, applying retention instructions and automating disposal. However, as

the latter has not yet been fully switched on within the system, it is not yet supporting the department to meet requirements set out in the Section 46 Code of Practice.

The effective operation of the system is being affected by issues around the process of 'checking in' and 'declaring' records within IWS. Staff do not always realise that they need to 'check in' documents created within or moved to IWS for it to be visible to others within IWS. This may in part be because checking in happens automatically when emails are moved across from Outlook to IWS (though the performance issues earlier in the year on occasions prevented this from happening). Staff also do not always understand the need to 'declare' documents as a 'record' for them to be managed as such. Once automated disposal is enabled within the shared resources area, information will be deleted after three years unless it is declared as a record. However, according to figures from the department's IT partner, Atos, only 6% of information within IWS has been declared as a record compared to around 80% record content in MEDS.

The department needs to ensure that staff understand when and how to 'check in' and 'declare' information. As well as supporting this process from a cultural, policy and governance point of view, the department should consider whether these issues can be circumvented through technical means. This might, for example, include exploring whether checking in and declaring records can be made a default option. **See Recommendations 1 and 3.**

IWS and the shared drives

Although IWS is the 'preferred place for managing documents', the department's draft IWS strategy emphasises that it is 'not yet sufficiently robust or scalable' to act as the sole records and information repository.

The connector between Outlook and IWS was upgraded in March 2014 and the department has worked with a contractor, Automated Intelligence, to develop a tailored 'non PST' version of SyncPoint, which it expected to roll out in December 2014. The assessment team understands that these steps may

only provide respite for about 12 months. The draft IWS strategy states that ‘insufficient capacity planning was done up front. As a result, the logical architecture has proven not to be robust over the long term’. Atos has been tasked with building a capacity tool based on Microsoft best practice to show the impact of data volumes on SharePoint. The draft IWS strategy indicates that options for a new logical architecture for IWS will be put forward to improve scalability.

As noted above, the department also has a number of shared drives and statistics suggest that their usage is increasing. The capacity review of IWS carried out by Atos revealed that the shared drives contain 5.4TB of information (which equates to 13.57 million files) and are growing by approximately 845GB per year (twice as much as IWS which is growing by 408GB per year). IWS is not being fully exploited, which is likely to be due in part to the performance issues in early 2014 and to business areas being familiar with and finding it easy to use shared drives.

The shared drives are not subject to central control and retention/disposal instructions are not being applied to them. A lack of reporting functionality means it is difficult to get oversight of what is on the shared drives and how they are being used. The draft IWS strategy establishes a goal of decommissioning redundant shared drives by December 2015, but this will remain an aspiration until IWS has been sufficiently stabilised and is used successfully by staff.

Although information stored within the shared drives cannot be ‘declared’ by staff as a record from a technical point of view, it may nonetheless have long-term historic or business value. If shared drives continue to be used there is therefore a risk that a significant part of the department’s record will remain unmanaged in a corporate sense and may not be available in line with business need or legal requirements, meaning that the time and money spent on bringing in IWS will have been wasted. Clear plans need to be put in place for the shared drives and the information they contain.

To support this, the department needs to continue to focus on improving the performance of IWS and better aligning it to user need. It has identified what it needs to do to address the technical issues within IWS. It now needs to prioritise this work and ensure that it is given sufficient support. Once IWS has been stabilised sufficiently, the department should 're-launch' IWS and mandate its use. **See Recommendation 1.**

Email and collaborative platforms

The department has imposed 300MB limits on Outlook mailboxes to encourage the regular corporate storage of email. Many staff interviewed stated that they struggle to keep within this limit and either deleted emails on an ad-hoc basis or moved large amounts of email into IWS to free up capacity. Within MEDS the ease of capturing emails (on sending an email staff would be presented with a dialogue box enabling them to save it across to MEDs) means that almost all of its 33 million records are email. The assessment team heard anecdotal accounts of tailored searches within the system turning up large volumes of 'Out of Office' replies. Within IWS, the 'dumping' of email was a major contributing factor in the system's performance issues. Atos figures show that between 80 and 90% of content is email.

The process of getting email into IWS is simple and effective (as demonstrated to the assessment team). All a user needs to do is set up folders in Outlook that are linked to corresponding folders in IWS and drag and drop emails across. This can be done for single emails and for batches. An impending update will also flag emails so staff can see which ones have been transferred to IWS.

The department hopes to introduce an email archive to provide some temporary back-up email storage, with the expectation that this will relieve pressure on Outlook inboxes. It is proposed that emails will be archived after 60 days, retained within the archive for a period of two years and then disposed of automatically. This report emphasises that while the current situation is far from satisfactory and while the introduction of an email archive

has the potential to ease the burden on staff and systems, it may also have an impact on the capture of information with corporate value. The existence of an archive will remove an incentive to move emails out of Outlook and may lead some staff to believe that they do not need to do so, for example, if automated rolling deletion is not recognised. Staff may also feel they do not have time to search the archive retrospectively to work out what information needs to be saved, may be content for emails to be deleted by the system or may simply prefer to keep emails within the archive. This might be the case if staff find corporate systems hard to search or are concerned about access to sensitive information. To mitigate this risk, the department needs to ensure that staff understand the purpose of the email archive, how disposal operates and what should be done with emails with corporate value. **See Recommendations 3 and 9.**

The department also rolled out in May 2014 a new collaboration system, DHeXchange, on the cloud-based collaboration platform Kahootz. The purpose of the system is to enable secure working with external partners. There are similar collaboration capabilities within SharePoint and it is hoped that these can be developed for internal collaboration in the future. The department needs to keep track of the information that is held within DHeXchange and ensure that record content is managed throughout its lifecycle, either within DHeXchange itself or by moving record content to IWS. **See Recommendation 1.**

Finding, accessing and protecting information

While the top levels of the filing structure within IWS are created and controlled corporately, LFMs are responsible for the development and maintenance of the lower levels of the file plan. According to the draft IWS Strategy, 'Evidence from reviews of the file plan … suggests that at lower levels, the folder structures are already complicated, deep and poorly thought out. Most are growing organically rather than in a planned and organised manner.' The customer insight survey (Autumn 2014) suggests that staff have difficulty understanding the way folders are organised and named. Staff have also complained that the 4 or 5 levels IWS is currently limited to, is not

sufficient for their needs and that a deeper file plan would make it easier for them to find information. This may reflect established working patterns in shared drives where file structures may be deeper and more complex. While such filing structures may support discovery for individual members of staff or particular teams, they will not do so from a corporate point of view. Good practice guidance suggests that a filing structure should not be more than four levels and it is recommended that the department follows this. It also needs to ensure that staff understand the filing structure, particularly the areas that they should be using. **See Recommendation 3.**

IWS allows staff to perform relatively sophisticated searches using a number of filtering options. Staff have been critical about the search functionality within IWS but the assessment team's view is that this is largely due to a lack of understanding about how they can refine searches. An initial technical issue where the search engine was not indexing all the required metadata fields has now been resolved.

IWS supports the automatic captures of some metadata. Staff are encouraged to add further metadata when they save a record to IWS but this is not mandated so it is unlikely that staff will invest the additional time needed to do this. The department needs to ensure that it is collecting sufficiently good quality metadata to aid retention, scheduling and management of its records, and ultimately meet requirements for transfer to The National Archives. **See Recommendation 5.**

IWS was introduced with an expectation that records would be open by default, but access controls can be added where necessary. This represents a substantial culture change for staff as access to MEDS and shared drives was largely limited to individual team areas. The KIM team and LFMs often have to field requests from staff asking for areas of the file plan to be closed. The KIM team must be empowered to push back to the business on these requests as necessary. If access controls are not applied correctly there is a risk that staff will be unable to access and share information as needed. The department must ensure that staff can understand when access controls are appropriate

and support the KIM team and LFMs in rejecting unnecessary requests to close files or folders. **See Recommendation 4.**

It is not yet possible to access IWS from mobile devices and this has led some staff to keep information in Outlook rather than IWS. There is a risk that staff will continue to work around IWS if they can't access it where and when they need to. As part of the work to improve and enhance IWS, the department should look at the possibility of providing mobile access. **See Recommendation 1.**

2.2 The continuity of digital information

IMA goal: The organisation is taking proactive steps to ensure the continuity of its information, over time and through change.

Understanding what information is held

The department does not have a complete picture of the digital information that it holds. In addition to its own digital information, a key challenge is represented by the significant amount of information inherited from more than 300 separate Primary Care Trusts (PCTs), Strategic Health Authorities (SHAs) and other organisations due to the structural changes within the wider Health Service. The department had no previous knowledge, control or oversight of these records and has subsequently undertaken a programme to take control of this information. It also recognises the importance of being able to search and retrieve records to support ongoing legal and other reviews. Although some work has been done to understand what is held at a macro level, there is some way to go before the holdings are fully understood.

There is no overall corporate understanding of what information is held on the shared drives, though individual teams may understand what their file structures contain. The IMA team saw no evidence to suggest that the department has fully mapped its technology environment.

At the same time as defining how its definition of an information asset should be applied to unstructured information, the department should seek to identify at a proportionate level what unstructured information assets its IAOs are responsible for and where they are held. **See Recommendation 2.**

Digital continuity and technology change

Some work has been done to bring the information received from PCTs and SHAs together on one platform. The next step is to migrate away from the NHS platform to a Department of Health platform. However, there is no plan yet to ensure the continuity of this information in the long term.

The department has allocated two staff to provide on-going technical support for MEDS. Although it will not be possible to migrate from Lotus 7 to a newer version as the bespoke functionality of the original system would be lost, the system has been stabilised within the current Microsoft environment. As such, there is no immediate need to migrate records out of MEDs and the system continues to support the on-going availability of information. This is **good practice**.

However, as with PCT and SHA records, there is no plan in place to ensure the long-term continuity of this information, including, for example, the migration of information out of MEDS should the department not be able to keep the system running. There is also currently no plan for a wholesale migration of information from shared drives to IWS, although staff are being encouraged informally to transfer material that is in active use. In this case, the lack of an overall plan to govern this approach means information of potential value may not be moved to IWS, and may instead be left on shared drives, becoming incomplete, unusable and unavailable.

The department should take steps to understand the risks around its digital information focusing on MEDS, the shared drives and the PCT and SHA records. In alignment to its overall information strategy it should devise a plan for ensuring that the information is complete, usable and available for as long

as it is needed. First steps should include running a tool like DROID over these information stores to get a sense of the age of the information and formats held and creating a plan for migration from the shared drives. This should detail what should be moved across, responsibilities and timings including when the shared drives will be closed down and when the remaining contents will be disposed of. It is also recommended that the department devises a plan for the possible migration of information from MEDS to a more sustainable system. **See Recommendation 5.**

3 Information risk, governance and oversight

3.1 Recognising information risks

IMA goal: The organisation defines and manages information risks to minimise threats and maximise opportunities.

Governance for information risk

The Director General of Group Operations and Assurance (GOA) acted as Senior Information Risk Owner (SIRO) from 2012 until her departure in March 2014. Following this, her role was overseen by the GOA Senior Management Team under the chairmanship of the Director, Estates & Corporate Information Services. SIRO responsibilities were within scope of these arrangements and were assumed by the Director, Estates & Corporate Information Services on an interim basis until 31 October 2014, when the role was allocated by the Permanent Secretary to the new Director General, Innovation, Growth and Technology (IGT). The DG IGT role was part of the role undertaken previously by DG GOA.

The assessment team note that the department has engaged with The National Archives on Information Assurance and Cyber Security training, including briefing sessions for the Audit and Risk Committee and the current SIRO. Senior interviewees indicated that the SIRO's responsibility for information governance and cyber risk policy across the NHS made the role a particularly good fit. This IMA report recognises the potential significance and impact of information risks that could arise within Arm's Length Bodies. However, it also emphasises that the potential magnitude of those risks must not mean that information risks within the core department are overlooked. The department must support the SIRO to gain oversight of all information risks and to assess how effectively they are being mitigated. Of particular relevance in the context of this report are risks relating to information and

records management, whose importance has been emphasised by recent enquires and the publication of the Alex Allan *Records Review* report.[3]

The Departmental Record Officer (DRO), who has responsibility for leading on compliance with the Public Records Act, is not included on the October 2014 information governance diagram supplied to the assessment team. The diagram also shows no link or dotted line between the new SIRO and the new DG of Group Operations (the Chief Operating Officer) or the Director Estates & Corporate Information Services. This report recognises that new governance arrangements were bedding in at the time of the IMA, but emphasises that the importance of the DRO needs to be recognised within the information governance structure and appropriate links made to the SIRO. **See Recommendation 6.**

Defining information risk and managing it

The department's current Information assurance policy and strategy is formally owned by the SIRO on behalf of the Board. It establishes the need for a proportionate approach to protecting information, defined by its sensitivity, criticality and value. The department also provides detailed guidance for staff on data loss.

In addition to setting out the role of IAOs and the need for regular risk assessments, 'Managing Information Risk' guidance highlights the need to recognise confidentiality, integrity and availability-related risks. It also prompts staff to be proactive and 'think about what the consequences of data loss or unauthorised use, errors or unavailability might be'. The guidance also highlights the benefits of transparency and the potentially significant impact of not sharing information when there is a need to do so. **This is good practice.**

A number of staff interviewed demonstrated a sound understanding of information risk in its widest sense. For example, one interviewee highlighted the potential reputational impact of bad practice in information management

[3] https://www.gov.uk/government/publications/records-review-by-sir-alex-allan

and stated that the key risk for them was ‘that knowledge is invested in the individual, leading to reworking and reinventing the wheel’. The assessment team also saw evidence that a number of interviewees recognised that such risks needed to be managed. One member of staff had taken action to agree retention periods for data held externally, following identification of a lack of control in this area. Another described a decision taken at a senior level to move away from shared drives because of concerns over business continuity and the ability to share information across team boundaries.

The Department of Health 2012 Risk Policy and Risk Management Guidance establishes the responsibilities for all staff in managing risk. It sets out the agreed system for escalation of risk to the Departmental Board via the Strategic Risk Register and the requirement for all branches, directorates, projects and programmes to maintain risk registers. The document does not explicitly reference information risk.

Individual risk assessments conducted by IAOs enable a range of information risks related to individual information assets to be raised. However, as the department lacks a single definition of an information asset that is consistently applied to all the information the department holds, this cannot provide a complete overview. In addition, while the information risk assessment includes questions on secure disposal and availability of information, it does not cover retention, or address potential risks relating to keeping information for too long or short a time, or of failing to capture the right information in the first place.

The Estates and Information Services risk register includes a risk relating to the effectiveness of IWS. Stated impacts include the use of alternative repositories leading to incomplete knowledge and access to records. While positive, this captures only one aspect of the risks that the department faces in relation to information and records management. It does not set out the full potential impact of the mixed shared drive and IWS environment or technical considerations such as the impact of the fact that automated disposal is not yet enabled. It does not set out the impact of cultural and governance causes including lack of clarity over information’s value or how the system needs to

be used, or the fact that IWS is not mandated in policy. Importantly, it also does not show how relevant risks are being addressed and what mitigating actions are being taken.

Above the level of the Estates and Information Services risk register, the departmental risk register recognises the threat that confidential personal or departmental data might be lost or made public. The risk description viewed by the assessment team does not include potential causes, and as a result the assessment team could not confirm whether the potential role of bad practice in information management in undermining information security is recognised at this level. It is clear, however, that the parallel threat of a failure to capture or keep the right information, in line with its value, has not been formally defined by the department at this level or beneath it. This gap must be addressed. This is crucial given the potential impact in terms of the department's ability to comply with legal requirements, justify or explain past actions and meet operational and strategic outcomes. Defining this risk would offer the opportunity to embed mitigating actions within the wider risk management framework at all levels including, for example, within project and programme risk management plans. **See Recommendation 6.**

This report also notes that the appointment of IAOs is positioned as a mitigating factor for the risk of data loss referenced above. The department should also place emphasis on the assurance they provide and risk assessments they carry out. **See Recommendation 6.**

3.2 Establishing control

IMA goal: The organisation has effective governance structures in place that foster communication and strategic planning.

Supporting the business

The DRO is the section head of the Records, Archive and Retrieval Service, which sits alongside the Knowledge and Collaboration Centre within the

Business Engagement Branch of Estates and Information Services under an SCS1 Branch Head. The Knowledge and Collaboration Centre has responsibility for administrating IWS and enacting permissions changes, managing folders and helping staff get set up in the system. The KIM team has estimated that support delivered has amounted to an additional 300–400 calls, visits and emails a year. This has been delivered within existing resources.

Workplace Operations, ICT Futures and Shared Services, and Policy and Advisory Branch are also located within the Estates and Information Services. Policy and Advisory leads on data protection and information assurance; security; business continuity management; and financial and business management. The assessment team saw evidence of informal working relationships that appear to have been facilitated by the co-location of IT, information assurance and knowledge and information management teams within the same directorate. There are additionally a number of boards and KIM-focused meetings in place including an IWS improvement board and a regular KIM engagement meeting. This is led by the Director Estates and Corporate Information Services and is attended by the DRO and Head of Information Assurance. It covers key operational considerations including progress of the internal IMA programme and planned LFM meetings.

The assessment team saw no evidence of any strategically-focused information boards set up to facilitate long-term planning. The department should review current provision of boards to enable strategic planning as well as operational governance. **See Recommendation 1.**

Networks

At the time of assessment, the department's LFM network numbered around 378 staff, who carry out required duties in addition to their substantive role. The role is IWS-focused and does not extend to the management of the shared drives. No LFMs interviewed recognised any responsibilities in this area. The department therefore should ensure that formalising requirements in relation to IAOs and information custodians, as recommended above, is

used as a means to help provide a supportive governance structure for the shared drives. **See Recommendation 2.**

A draft LFM objective summarises their responsibilities as follows: ‘To foster and support the use of Information Workspace through effective folder management, communications and access management for x team/division/directorate’. This is expected to extend beyond administration of the system to taking an active part in the LFM community, encouraging good practice and acting as a conduit for guidance and communications from the IWS team.

None of the LFMs interviewed appeared to view the role as a burden, but opinions varied on the extent to which LFMs should be policing use of the system or challenging bad practice. The assessment team found that there was a lack of consistency in the role of the LFM. In some cases, LFMs are able to be very proactive, with one interviewee stating that they had undertaken spot checks under their own initiative and tried to obtain system usage statistics for their team to provide further leverage. In other cases interviewees indicated that the role was more about filing for colleagues, though the role description explicitly states that it does not involve this activity. To help address this, the department should ensure that policy and guidance provide clarity on who has responsibility for capturing information. In wider terms, this is also important because of the potential role that a lack of clarity in this regard may be playing a role in the duplication and dumping of email. **See Recommendation 9.**

LFMs are supported centrally through a quarterly ‘Why Information Matters’ newsletter. The autumn 2014 edition gave the dates of forthcoming training sessions, IWS news stories relating to forthcoming updates and improvements, requests for feedback, systems-related features and case studies. The department also holds regular sessions for LFMs, one of which the assessment team had the opportunity to attend. This was the third held in 2014, each session being offered at a number of dates, times and venues to help maximise attendance and participation. LFMs interviewed indicated that

they found the sessions helpful and the assessment team found the session to be of good quality, offering an opportunity to promote priorities and quick wins and to address questions and concerns. Concerns raised by attendees included the lack of emphasis that some teams were placing on information management and difficulties leveraging change. **This is good practice**.

This report recognises the impressive amount of effort that is being invested in the LFM network. However, a considerable weight is placed on it in terms of driving the proper administration of the system and in supporting business outcomes by making sure staff can get the most out of the system. The department needs to ensure that the LFMs continue to be provided with clear direction and, just as importantly, needs to ensure that they are empowered and supported to do their job. As a first step, the department should formally embed the draft LFM objective within the performance management framework and ensure that good performance is recognised in that context. The department should formally recognise and promote the role of the LFM network in mitigating information risk and define how the network supports IAOs in this regard. **See Recommendations 2 and 7.**

3.3 Providing direction

IMA goal: The organisation gives staff the instruction they need to manage, protect and exploit information effectively.

Knowledge and information management policy and guidance

The development of the five principles of information management and the links between information and records management policies and the information assurance policy and strategy put the department in a good position to deliver a consistent message to staff. The assessment team notes that the recent review of the intranet has placed the policy within a generic 'How to …' section, alongside other corporate requirements, which is a positive step.

However, the assessment team also notes that the main information management policy has now been broken into a number of discrete web pages, without being revised or substantially rewritten. The foreword by the Permanent Under-Secretary is now displayed in plain text format without prominence within the first set of pages and is not cross referenced, linked to or otherwise highlighted within the remainder of the pages. This reduces the benefit of this valuable endorsement. The policy's tagline, 'Collectively responsible – personally accountable', which was originally highlighted within the Permanent Under-Secretary's foreword, has also been removed. The department's digital and information and records management teams should work together to ensure corporate policy is displayed to best effect so that key principles and mandate are communicated effectively and reinforced. **See Recommendation 3.**

Information management policy is supported by a further set of pages offering records management related content. Tailored, system-specific guidance is also available via a 'support' tab in IWS. This covers the basic actions staff need to carry out, such as creating and moving documents, connecting to IWS in Outlook and Windows, working in Outlook and using views and filters to help find information. It also includes guidance on declaring a record within IWS and provides advice under a 'best practice' heading on creating folders, the difference between shared resources and team areas, guidance on what constitutes a record (see below, pp. 42–3) and sample IWS protocols.

There is an expectation that teams should produce these protocols to define how they work with IWS and the records team also offers a template shared drive protocol, which is available on request, but is not published. The existence of protocols is checked during internal IMAs, but the assessment team found no formal requirement within corporate policy to establish them.

Based on interviews with staff and the high volume of email saved within IWS, it is likely that a significant number of staff only interact with IWS via Outlook and rarely if ever enter the system. Staff may therefore be unaware of the

advice or instruction that is available to them within IWS, including in key areas such as records declaration. The department should ensure that such guidance is also available via the intranet. Repositioning it as 'How to …' guidance rather than 'support' may also increase its profile. **See Recommendation 3**

The information management policy establishes the following points in relation to ownership of shared drives by business areas:

- ensuring that their shared drive structure is relevant, appropriately labelled, and meets business need;
- putting processes in place to regularly review and delete old material;
- ensuring any sensitive information stored on shared drives carries the appropriate security classification, a clear handling instruction, and that appropriate access controls are applied;
- implementing document naming and versioning conventions;
- when the time comes, working with Estates and Information Services personnel to migrate relevant documents into IWS to enable the close down of the shared drive.

Although these points are positive, the information management policy does not provide a concrete statement on what the shared drives are actually for, or how staff should use them in relation to IWS. The records management pages on the department's intranet list Contact, BMS and IWS as the three main systems in which records are kept, without referencing the role of the shared drives. In addition to being unclear, the current line may also be giving the impression that anything stored in locations such as the shared drives is not a record and therefore by definition lacks medium- to long-term business or historic value. The contents of the shared drives will therefore not simply consist of redundant information that is duplicated elsewhere. Although policy establishes IWS as the preferred location for storing records, in practice, information is likely to have been stored in the shared drives out of preference and not because it lacks value in either sense. The above requirement to 'regularly review and delete old material' is a particular concern because of this and the lack of corporate oversight and control of the contents of the shared drives. **See Recommendations 3 and 9.**

One member of staff indicated that information within their shared drive dated back to 2006. Others described information stored within the shared drives as a core and valued resource, stating that they represented the 'institutional memory of the team' or said 'everything goes on the shared drives – you soon get complaints if it doesn't'. Varied practices were evident, with staff suggesting that colleagues had reverted to using shared drives following the introduction of IWS, and one referencing a team where half the members were using the shared drives and half were using IWS. Two separate LFMs gave their view that staff would continue to use shared drives until they were explicitly told not to.

As well as looking at how it conveys key messages in relation to IWS use, the department must provide a clear and promoted policy line for staff, managers and IAOs that states how shared drives should be used. This should be incorporated within the department's strategic approach for its information and should be reviewed and updated as necessary. Its application should also be monitored. **See Recommendations 1 and 3.**

Deciding what information needs to be kept

The department's retention and destruction policy is intended to be published on GOV.UK, which represents **good practice**. It contains the department's retention schedule, which is also available to staff via the records management pages on the intranet. These pages also provide the following definition of a record:

> A record is any piece of information that has future value and allows us to:
>
> - support our legal requirements
> - provide evidence of an action endorsed by ministers or a important management or operational decision (eg commitment of resources)
> - provide evidence of a change in policy and describes:
>   - who was involved in the decision-making
>   - why something was accepted or rejected

- whether the decision is directly relevant to the success or failure of an activity.

The department states that records may be classified under three headings: administrative, operational or historic. This definition is duplicated in the IWS support pages, with an additional statement that records are created by placing emails, digital documents and files in IWS, and that 'all records are stored in Shared Resources'. Although there is a link to a page titled 'how to declare documents for the record', this may, like statements in the information management policy, suggest that a record is a record because it is stored in IWS.

Although this definition contains a number of positive elements, it is likely to be insufficient by itself to help staff understand what they should be keeping. A number of interviewees were particularly concerned on this point. One member of staff highlighted a lack of clarity over responsibility for capturing the record relating to policy decisions that were being discussed with Arms-Length Bodies. Another senior member of staff told the assessment team:

> 'I am not clear what information we are expected to save or the processes to support us to do this – it's all a bit of a mess. If I asked my team what information needed to be saved I'd get different answers from each of them. I'm not sure there is any guidance – you can't just expect people to know what to do, you need to tell us. The department needs to think about what to keep and why and engage people so they care about it.'

The department needs to ensure that staff have ready access to clear principles. The current lack of promoted and practical guidance on 'What to Keep' is likely to increase the threat that information is not captured or kept in line with its value. At an organisational, team or individual level, a lack of clarity in this regard may lead to the inadvertent retention of large volumes of information with little or no value, or the loss of information with business or historic value. A lack of defined principles also makes it harder to prevent

deliberate decisions not to document decisions or dispose of information that needs to be retained. **See Recommendation 9.**

Providing training

The department offers a mandatory two-hour induction in knowledge and information management, which reportedly consists of a mixture of practical demonstrations, presentations and culture-focused case studies. The department also provides an introduction to IT course, 'IWS basics' training for all staff, and IWS training for LFMs. The IWS basics course is 'highly recommended' rather than mandatory. Although this course is reportedly promoted through the introduction to IT and LFM IWS training, an estimated 30–35% of staff have not received any training in the system. The department needs to ensure that all staff who need to use IWS receive instruction in how to use the department's preferred repository for digital records. This may, for example, be leveraged through IAO reporting. The department should also ensure that all new staff are provided with a corporate statement on the use of shared drives to enable them to comply with the information management policy. **See Recommendation 3.**

This report notes the department's commitment to promoting online 'Responsible for Information' training, with a Board-level presentation delivered to establish its priority. Interviewees indicated that the importance of completing the course, or ensuring staff did so, was recognised. In addition to this, the department has also run a separate 'Secure Information' campaign, which further demonstrates its commitment to conveying importance of information security. The core messages of the campaign were delivered through a variety of channels including video clips on the intranet and hosted on YouTube, postcards and posters. The assessment team understand that in parallel with this campaign, compliance checks were run on the department's clear desk policy.

At the time of assessment, early planning was underway for a linked 'Storing Information' campaign to be run in early 2015. This was expected to focus on how to store information, who to share it with and how to manage it

effectively. This provides an excellent opportunity to convey core messages in relation to IWS use, but must also cover key requirements for structuring and storing information in shared drives as well as key principles on what information to keep. **See Recommendation 9.**

3.4 Measuring impact

IMA goal: The organisation measures performance in practice and takes informed risk-based action as a result.

Measuring compliance with policy

The department has established its own internal programme of assessments to monitor compliance with the information management policy, a key requirement under the Section 46 Code of Practice. The department positions these assessments as a means of identifying and resolving through guidance weaknesses in information management process. The 'Why Information Matters' newsletter reviewed by the assessment team indicates that the department's KIM team completed two first assessments, three reassessments and five annual assessments between June and October 2014. The newsletter highlighted the significant progress made by one particular team and includes a case study setting out what work had been done to achieve the improvement.

A sample report provided to the assessment team shows that business areas are provided with quick wins and longer-term recommendations. Outcomes since the previous assessment are considered when an area is revisited. Performance of business areas is measured against 61 criteria distributed against the five policy headings and an additional heading covering training and awareness. Although recommendations place an emphasis on encouraging rather than mandating, it is clear that the department is using the process to target identified priorities and concerns such as email storage. It is also clear that, in line with the department's inclusive information

management policy, the focus of the process is wide. Questions extend to cover the promotion of transparency outcomes, knowledge capture and exit processes, access to calendars and the maintenance of Directory entries. **This is good practice**.

While strongly supporting the department's proactivity in establishing the internal assessment process and in maintaining it through the recent period of organisational transformation, this report notes that assessments are not mandatory and that results are not published to the department. There are also minimal links with the separate information risk assessments and consideration could be given to creating stronger connections between the two. The internal assessment process also appears reliant on input from KIM leads within the business. In line with this report's recommendations, the department's internal assessment process should be empowered to tackle key risk areas and place a more detailed focus on the structure and use of IWS and the existence and promotion of 'What to Keep' guidance. A current gap is the lack of coverage of how shared drives are used and structured and how each business area's information is distributed between shared drives and IWS. The above points should be addressed, and the assessment process should be expanded to incorporate key comparable quantities and qualitative measures. **See Recommendation 8.**

Assessing progress against strategic goals

Once the department has fully defined its strategic approach and vision post-2015, a schedule for reporting must be agreed so that the department's senior team can assess what progress is being made to reduce threats and increase opportunities. **See Recommendation 1.**

4 Records, review and transfer

4.1 Oversight of records and selection

IMA goal: The organisation understands the value of its records and can consistently identify those with enduring historical value.

Oversight, control and use of records

The DRO role sits within the Estates and Information Services Directorate and has a team of 12 based largely in Burnley, though they regularly travel to the department's other offices in London and Leeds. The DRO works closely with the Knowledge and Collaboration Centre team on current information management tasks.

The assessment team is concerned that the DRO is currently somewhat stretched, in part because of the need to oversee PCT and SHA records. The department needs to ensure that the DRO role reflects in practice the outcomes set out in The National Archives' guidance on the DRO role, and that the DRO is given sufficient support to carry out these tasks.

In addition, the assessment team notes that the retention and destruction policy states that the records management team does not implement retention decisions on information assets, or information held elsewhere including shared or personal drives. In view of the DRO's overall responsibility to ensure all information is managed from creation through to destruction or transfer, the department should ensure that arrangements in these cases are made explicit in this policy. It should ensure that disposal scheduling is covered within the IAR to help provide the DRO with assurance that necessary arrangements are in place. This should also be considered when reviewing the DRO's position within information governance arrangements and role in supporting the SIRO. **See Recommendations 2, 6 and 9.**

Appraisal and selection

A team of two staff is responsible for the process of appraisal, selection, sensitivity review, listing and transfer to TNA. Historically, the department has performed the appraisal, preparation and transfer of paper records to a high standard. Records Transfer Report figures published by The National Archives (Autumn 2014) show that steady progress is being made with appraisal and selection of records.[4] It is also clear that figures have been refined and improved over time.

The department's established practice of recalling paper files for appraisal 25 years from the date of creation has meant that it has avoided building up a large backlog of legacy files. The review team has started to try, in line with The National Archives' advice and guidance, using macro appraisal methods for paper records using file titles and selection criteria to sift files, with the hope that this will speed up the process of appraisal and increase efficiency. The department is also researching prefixes, and using patterns of what has and has not been selected previously, to aid decision making. This is **good practice**.

The department has not yet developed an approach or plan for the appraisal of digital information. There are some indications that MEDS records were poorly kept and managed, which will make appraisal extremely difficult. For example, the department conducted a trial to identify records of historical value within MEDs that focused on locating management board records. It proved impossible to find a complete set within the system.

It is hoped that the application of retention periods to IWS will make appraisal of records within that system easier in the long term. As yet, there are no plans to appraise material on the shared drives. Although the department is not due to transfer digital records to The National Archives until around 2020, early flagging of records of historical value will help to ensure they are protected and survive through to the point of transfer. The department needs

[4] http://www.nationalarchives.gov.uk/about/record-transfer-report.htm

to draw on The National Archives advice and guidance and the experience of other government departments in digital appraisal to devise a plan and approach that works for them. It needs to ensure that this covers all digital information, not just those in MEDs or IWS and includes digital information transferred from PCTs and SHAs. **See Recommendation 10.**

The department has taken in almost 475,000 boxes of paper records from PCTs and SHAs in addition to the 19 million digital records referenced above (see p.30). These records are not reflected in the department's Autumn 2014 Records Transfer Report return. While these records are unlikely to be selected for transfer to The National Archives, they still need to be appraised and any records of local interest transferred to the appropriate local repository. The DRO and his team will be responsible for management of these records in the immediate term and for the appraisal, selection and disposal of these in the long term. There are plans to recruit extra resource to help with this work but so far this has not happened. If the department is to meet its obligations it needs to ensure that additional resource is brought in as planned, and that these records are factored in as part of their wider plans for the management of their paper records. **See Recommendation 11.**

4.2 Implementing disposal decisions

IMA goal: The organisation understands the process for records disposal and consistently implements decisions in line with defined plans.

Triggers for disposal

Both MEDS and IWS support the automated setting of retention periods and disposal of information. The department has applied retention periods to MEDS and is actively disposing of records once their retention period has ended. The DRO is responsible for activating disposal on a regular basis. This is **good practice**. A total of 76,000 documents held on MEDS were destroyed between December 2014 and December 2015, with destruction due to be

undertaken on a further volume of records once requests for information to support statutory inquiries and reviews have been completed.

Within IWS, a trigger date is added to folders to activate disposal; this is the responsibility of the LFMs. This is **good practice**. As the system has been in place for more than 18 months, the earliest records in this team area will soon be due for disposal. Many staff either do not realise that some material will soon be deleted or are unclear when or on what basis automated disposal will take place. The assessment team also heard anecdotal advice that staff are being advised to check out records that they need to keep for longer and then check them back in again to reset the clock. As noted above, if records within the shared resources area are not 'declared' as records then they will in principle be disposed of after 3 years, rather than inheriting an appropriate retention period from the section of the file plan in which they reside.

There is a risk that the good work that the department has done around identifying and applying broad retention periods to IWS will be wasted if disposal is not carried through to conclusion. The department should prioritise increasing understanding of what information needs to be kept, and what needs to be done to make it a record, together with work to ensure disposal happens in practice. Direction for both should be provided by the department's information strategy. **See Recommendations 1, 3 and 9.**

Sensitivity review and planning to transfer

Transfer of material to The National Archives has been delayed due to confusion about the application of FOI exemptions to medical information of individuals. The assessment team were told that there was conflicting advice on the correct application of FOI exemptions as they applied to historic records. The department is closing more of this material, leading to an increased number of redactions, which has reportedly proved extremely time-consuming. The department also raised concerns about the time required to get approval for closures from the Lord Chancellor's Advisory Council.

The department has not yet explored processes for the sensitivity review of digital information, but it is expected that past filing practices may make this difficult. This report recommends that the department works closely with The National Archives to agree a workable solution for the closure and review of sensitive information. **See Recommendation 10.**

Glossary

AI – Automated Intelligence

ALB – Arms-Length Body

Atos – Department of Health's IT partner

BMS – Business Management System

DHeXchange – Department of Health's collaboration system

DRO – Departmental Record Officer

DROID – The National Archives' free tool for Digital Record Object Identification

ECM – Enterprise Content Management

FOI – Freedom of Information

IAO – Information Asset Owner

IAR - Information Asset Register

ICT – Information and Communications Technology

IT – Information Technology

IWS – Information Workspace, Department of Health's enterprise content management system

KIM – Knowledge and Information Management

LFM – Local Folder Manager

MEDS – Department of Health's bespoke electronic records management system

NHS – National Health Service

PCT – Primary Care Trust

RTR – Records Transfer Report

SHA - Strategic Health Authority

SIRO – Senior Information Risk Owner