

# **Annual Governance Statement for the year ended 31 March 2014/5**

## **Introduction and context**

The Health and Social Care Information Centre (HSCIC) is an executive non-departmental public body (ENDPB) established in April 2013 by the Health and Social Care Act 2012. It is responsible for setting up and operating systems for the collection, analysis, dissemination and publication of information relating to health services and adult social care. It is also the authority for determining and publishing information standards for health and adult social care in England. The HSCIC may also be directed by the Secretary of State for Health or the NHS Commissioning Board (NHS England) to provide system delivery functions in relation to the development or operation of information or communications systems concerned with the provision of health services or adult social care in England. The HSCIC is accountable directly to Parliament for the delivery of its statutory functions described within the Health and Social Care Act.

In line with the Department of Health's (DH) governance requirements of its arm's length body organisations, quarterly accountability meetings are held between the Chief Executive of the HSCIC and the Department of Health sponsor team to review the discharge of their accountability responsibilities which are set out in the Framework Agreement between the HSCIC and Department of Health.

Strengthened governance controls have been evident during 2014/15 through the information gathered via the quarterly statements of internal control reports and the programme of internal audits. The expectation is for this progress to continue and for the governance and control structures to become even more firmly embedded during 2015/16.

Examples of the developments made include the establishment of an Information Assurance and Cyber Security Committee, chaired by a non-executive director, reporting to the main Board, the development of an Assurance Map, improved reporting of key performance indicators to executive management and the main Board and risk management, both confirmed by audit, and the establishment of a Quality Council to review and monitor the effectiveness of the implementation and maintenance of all accepted standards, such as those of the International Organisation for Standardisation (ISO).

Despite the good progress being made in many areas, following concerns raised by the Health Select Committee, the HSCIC Board requested that a review be carried out of all data releases approved, including those authorised by the HSCIC's predecessor organisation the NHS Information Centre, to ensure proper governance had been applied in authorising the release of information. The independent review, overseen by Sir Nick Partridge, a non-executive director, reported in June 2014 with recommendations for strengthening governance and control in this area. These recommendations have since been taken forward.

The concern reported in the 2013/14 Governance Statement over the quality of accounting information on assets transferred from the Department of Health to the HSCIC has been addressed. ***DN. Need to ensure that this correlates to any references to this elsewhere in the Annual Report in sections provided by Finance.***

### **Scope of responsibility**

The HSCIC is responsible for maintaining a sound system of internal control that supports the achievement of its policies, aims and objectives whilst safeguarding public funds and the assets for which it is accountable, including data and information, in accordance with the requirements of *Managing Public Money*.

Throughout the year, the Accounting Officer and HSCIC Board have sought to exercise these responsibilities by establishing visible and effective systems of internal control and governance. The Senior Departmental Sponsor for the DH (Sponsor) is responsible for ensuring that the HSCIC procedures operate effectively, efficiently and in the interest of the public and the health sector.

### **Organisational Developments**

A new chief executive and team of non-executive directors joined the organisation on 1 April 2014 and further executive appointments have been made during the year. A Senior Independent Director was appointed in April 2014 and a new non-executive chair of the assurance and risk committee was appointed in September 2014.

As new executive directors have been appointed, responsibilities have changed amongst the executive team.

### **The governance framework**

The establishment and constitution of the HSCIC is set out in Schedule 18 of the Health and Social Care Act 2012.

The HSCIC is led by a Board consisting of non-executive and executive members and is the senior decision making structure in the organisation. It is accountable to the Secretary of State for Health and to Parliament.

The organisation is managed on a day to day basis, by an executive team led by the Chief Executive who is the Accounting Officer and is accountable to the Secretary of State and to Parliament for the performance of all functions and for meeting the organisation's statutory duties.

In operational terms, accountability is to the Senior Departmental Sponsor in DH. The formal arrangements are set out in the Accounting Officer Memorandum sent to the Chief Executive of the HSCIC by the DH Accounting Officer. They are also reflected in a Framework Agreement which governs the relationship between the HSCIC and DH.

Board members have a corporate responsibility for ensuring that HSCIC complies with all statutory and administrative requirements for the use of public funds. Details of the conduct of the Board and the roles and responsibilities of members are set out in the HSCIC Standing Orders, Standing Financial Instructions and Code of Practice for board members, which were reviewed during the course of 2014/15.

The HSCIC Board is assisted in carrying out its duties through an operational governance structure comprising the:

- **Executive Management Team (EMT):** responsible for communicating and delivering the overall strategy for the HSCIC (as agreed by the Board) and agreeing policy and procedures whilst supporting implementation. The group meets weekly with action points and decisions disseminated to all staff via the corporate intranet
- **Programme and Service Delivery Board (PSDB):** focussed predominately on the provision of corporate level assurance of all programmes, projects, services and corporate and statutory services (the HSCIC Portfolio), ensuring the HSCIC Portfolio is delivered within agreed tolerances, to associated delegated authorities and to appropriate standards. Where exceptions arise PSDB provides a mechanism for resolution.
- **Corporate Assurance Panel:** ensures that items requiring approval or endorsement by the Accounting Officer or Board meet the delegated approvals contained in the HSCIC Standing Financial Instructions and quality standard expectations of the organisation.
- **Transformation Programme Board:** owned the internal organisation development strategy and plan and ensured consistency across directorate transformation projects, until it was absorbed by EMT in June 2014 to ensure full alignment with executive management.

## HSCIC Board and Committee structures

The Board has responsibility for defining strategy and determining resource requirements to ensure the delivery of the HSCIC's objectives. The composition, role and main activities of the Board and its principal committees are detailed in the Annex.

In addition to standing agenda items on the governance and performance of the organisation, the Board discussed a range of topics including the:

- Development of a strategy and business plan in the context of a rapidly changing health and care system and a tight financial regime.
- Governance and structure of the HSCIC, led by an increasingly integrated internal transformation programme.
- Links and relationships with key stakeholders including NHS England and the Department of Health Sponsor.
- Monitoring of a broad range of performance indicators throughout the year which are aligned with the approved strategy and business plan. This included a refreshed and updated board performance pack.

In 2014/15 a Board effectiveness and governance review internal audit was undertaken. This did not highlight any significant issues or concerns that required immediate action or impact on the content of the Governance Statement ***DN. To be confirmed.***

The inaugural meeting of the HSCIC Information Assurance and Cyber Security Committee (IACSC) was held on 13 May 2014. The IACSC was constituted to ensure that there is an effective information assurance function that provides appropriate independent assurance to the Chief Executive and the Board.

The work of the Assurance & Risk Committee (ARC) has developed over the year. The key areas it addressed in terms of assurance and risk included:

- oversight of the 2013/14 annual accounts preparation for the HSCIC and recommending the approval of the final accounts to the Board
- review of the content of the draft annual governance statement
- oversight of the annual accounts preparation process for 2014/15
- strategic steer on and input to the internal audit strategy and annual plans in the context of the Department of Health's shared service agenda
- review of the internal audit reports and monitoring of implementation of associated recommendations
- review of the local counter-fraud specialist work-plan
- review of the external audit strategy
- monitoring of the management of the corporate risks and issues
- development and implementation of a corporate assurance map
- consideration of the ARC meetings arrangements to ensure efficiency and effectiveness.

The HSCIC complies with the central government corporate governance code as far as is relevant. No material departures have been identified.

### **Corporate governance**

Corporate governance assurance is provided by means of a quarterly Statement of Internal Control against criteria laid out by DH, which is approved by the Chief Executive and delivered to the DH Senior Departmental Sponsor. An Assurance Map has been developed which provides assessments of the assurance in place across the organisation and against the strategic risks, using the Three Lines of Defence Model, and has been used in developing the internal audit programme for 2015/16.

Corporate policies are reviewed on annual basis and the annual exercise to ensure that staff are aware of the HSCIC's confidentiality policy requirements and that conflicts of interest are declared has been carried out.

### **Key relationships**

The HSCIC does not work in isolation. It is part of the new health and care information system created by the Health and Social Care Act 2012 and works in collaboration with national partners. The Act placed a duty on all national arms' length body organisations (ALBs) to work

collaboratively in the interests of the system as a whole. This includes other national ALBs, commissioners and providers, local NHS organisations and local authorities.

A Customer Relations directorate under the leadership of a new executive director has been established in order to build strong customer and stakeholder relationships which enable the HSCIC to support those customers and stakeholders in delivering high quality services for patients and the public. Plans are in development to set up revised stakeholder and customer management, including strategic account management for key customers such as ALB's like Public Health England and the Care Quality Commission (CQC), and customer sectors such as commissioners of health and social care services and medical research. The way the HSCIC works alongside industry will be critical to our success and the management of these relationships is also being considered

Executive leads have been assigned to our important stakeholders. Existing relationships with Monitor, CQC and the NHS Trust Development Authority have been maintained and are being revitalised through strategic executive level discussions between the organisations.

The HSCIC is a key member of the National Information Board (NIB). The Chief Executive is a member of the NIB's Leadership Group, and all members of the Executive Management Team are involved in one or more of the NIB's working groups. We recognise the importance of the NIB and have contributed to the NIB's Framework for Action. Many of the commitments in the Framework relate directly to the HSCIC's statutory role, and we have therefore invested a lot of time and energy in ensuring that there is alignment across the NIB Framework and the HSCIC's strategy.

## **Performance management**

Corporate performance management is integrated with business planning and risk management in order to provide a joined-up view of:

- what the organisation intends to deliver (business planning);
- factors that could prevent successful delivery, and mitigation of these (risk management); and,
- how well the organisation is delivering (performance management)

In order for the HSCIC to be successful and deliver its statutory obligations and commitments to stakeholders an organisation-wide performance management framework has been designed. This framework includes the following elements:

- Key Performance Indicators (KPIs) reported in performance packs at HSCIC Board, EMT and directorate level. These performance packs contain a mix of financial and non-financial performance information, key risks and issues, and assessment of delivery against strategic commitments. Each KPI has a designated owner whose primary role is to be accountable for delivery of KPI targets. KPI owners must escalate any serious or recurring problems which require resolution.
- Monitoring of business plan delivery at corporate and directorate levels, reported quarterly at HSCIC Board, EMT and directorate level. Each business plan deliverable has a designated owner whose primary role is to be accountable for delivery of that deliverable.

- Performance reporting of other key work at HSCIC Board, EMT and directorate level, such as cyber security, organisational development and transformation, innovation and burden reduction.

With the exclusion of a few business confidential indicators, all of the performance framework is reported to public meetings of the HSCIC Board and is available on the HSCIC website. In this respect they support open and transparent governance and constitute an important channel of public accountability. Performance packs and business plan monitoring reports also inform quarterly accountability meetings between HSCIC and the Department of Health.

An HSCIC Performance Management Community has been established to provide an internal professional network and source of expertise. Its main purpose is to drive and support continuous improvement in performance management capability. Its objective is to ensure that performance management is embedded in good management behaviour and underpins sustainable and resilient delivery throughout the organisation. An internal audit review reported during 2014/15 found good practice in the development of the HSCIC's performance management arrangements.

Existing performance indicators are reviewed regularly to ensure they are meaningful and effective. New performance indicators will be introduced where required by changes to strategic priorities or operational activities. During 2015/16 we will continue to develop, enhance and embed corporate performance management arrangements to ensure they remain effective and fit for purpose.

## **Risk management**

An updated single policy, strategy and framework for risk management in HSCIC were introduced in early 2014/15 and a corporate risk manager was appointed during the year. A key element of the improvements in 2014/15 has been focused training and communications activity to enhance risk management capability and awareness.

A review has commenced to enhance the useability and functionality of the current risk data repository and the process of migrating all users not currently using the tool has continued. A data cleanse exercise and an ongoing quality assurance programme have been carried out to ensure that the risk information held is current, accurate and of good quality.

A refined corporate risk management KPI has been introduced to focus on the outcomes of our risk management effort and is being reported to EMT and the Board. The use of risk management performance metrics is starting to drive an overall improvement in risk data quality and risk management behaviours.

A Risk Management Forum has been established to act as the HSCIC risk management community of interest, with its main objective being to improve risk management capability, so that management of risk becomes embedded behaviour, which underpins organisational sustainability and resilience.

Risks are reported regularly and escalated through the internal governance structure with the top corporate risks and issues ultimately being considered at the Board, EMT, ARC and by the Sponsor. There has been a significant improvement in risk management within the organisation although it is acknowledged that the new processes and practices need some further time to bed in fully.

The most significant risks faced by the organisation through the year related to:

- Delivering on our statutory and legal obligations.
- Protection of data and cyber security.
- Safe collection, analysis and dissemination of high quality and timely data and information, which meets customer expectations.
- Demonstrating delivery of benefits from the programmes and services we offer.
- Securing an appropriate workforce.
- Maintaining operational continuity of systems and infrastructure we are charged to deliver.
- Securing a positive, responsive and trustworthy reputation and maintaining effective relationships with stakeholders.
- Design and delivery of systems that work or deliver as anticipated.

These risks were mitigated by:

- working with our sponsor team to ensure we are meeting our statutory and legal obligations.
- establishing industry-recognised practices (e.g. mandatory staff training, controls around data access, movement and destruction); and establishing a cyber security programme.
- contributing to, and implementing the recommendations of, the Information Governance Assurance Review and Partridge reviews (the latter related to data releases by the NHS Information Centre, a predecessor organisation).
- improving planning, forecasting, benefits and performance management capabilities, reporting quality and promoting a culture that encourages openness.
- undertaking a zero base review of finances and resource requirements, the continued implementation of a Transformation Programme and targeted recruitment activity to ensure we have the people and skills to meet our commitments.
- maintenance of robust infrastructure (e.g. high-availability networks, dual-site data centres, a single approach to service management, testing of Business Continuity plans).
- customer and stakeholder relationship management activity to ensure HSCIC supports them in delivering high quality services.
- development of technical governance structures and information governance standards.

During 2015/16, risk management will be developed in the following areas:

- the corporate strategic risk set, defined in 2014/15, will be further refined, assessed and appropriate mitigating actions taken.
- the HSCIC risk appetite will be further developed and communicated throughout the organisation.
- the risk KPI will be further refined to focus on the effectiveness of the outcomes of risk management effort.
- the continued delivery of the targeted risk management improvement plan, including improved tools, metrics, reporting and collection methods and enhanced EMT, ARC and Board visibility of, and confidence in, the organisation's risk management capability.

- the exploration of options for a more integrated approach to risk and assurance activity, using a risk based approach to focus assurance activity on the most significant areas of risk.

## **Information governance**

Within the HSCIC, the importance of having robust information governance procedures in place which are consistent across the organisation is fully recognised by the Board. This is a fundamental consideration for work the HSCIC has been commissioned to deliver such as the care.data programme and the insourcing of SPINE2.

During 2014/15 the governance responsibilities of the HSCIC have been expanded to provide system wide advice on operational information governance across the health and social care sectors. This is separate from its principal role of guardian of data which is set out in the Health and Social Care Act 2012.

The HSCIC has published its Code of Practice on handling confidential information in line with the Health and Social Care Act 2012 s.263 and has published a Guide to Confidentiality, which complements the Code. Both are aimed at the entire health and social care landscape.

The HSCIC now hosts the Information Governance Alliance which brings together expertise from across health and social care to act as the primary point of contact for authoritative advice and guidance to the wider system.

A further example of this system-wide remit is that a Caldicott Implementation Monitoring Team was established by the HSCIC to provide support to Dame Fiona Caldicott's Independent Information Governance Oversight Panel (IIGOP) by monitoring and reporting on implementation of the recommendations from Dame Fiona Caldicott's Information Governance Review. The outputs were reflected in the IIGOP's annual report published in January 2015.

A number of innovative cyber security projects will run alongside the HSCIC's Cyber Security Programme with the objective of benefiting the entire health and care system in the following ways:

- Establishment of an authoritative national focal point and governance model for care system cyber security guidance and incident support;
- Development of a 'scenario assist' package with relevant supporting products that would be made available to all care organisations and business partners to help guide their actions for cyber preparation, assurance and incident response; and
- Establishment of a strategic cyber risk oversight capability that will provide situational awareness monitoring of active risks such that scale is understood and early mitigations are possible.

The recommendations in Sir Nick Partridge's report, referred to above, have been fully embraced and progress has been made on each as follows. The HSCIC:

- has undertaken a programme of work to ensure that data has been deleted appropriately where the Data Sharing Agreement has ended.

- has developed one clear, simple, efficient and transparent process for the management of all data releases.
- is implementing a robust audit function, which will enable ongoing scrutiny of how data is being used, stored and deleted by those receiving it.
- has published its policy, process and governance for the release of data.
- has ensured there is clear, transparent and timely decision making, via the appropriate governance for all data releases, and that all decisions are documented and published on its website.
- has implemented a robust record keeping approach and the details of all data releases (including the purpose for which they are released) have been made available on its website.
- has developed one Data Sharing Framework Contract (DSC) and one Data Sharing Agreement (DSA), which is used for all releases of data, and which includes clear sanctions for any breaches.
- is actively pursuing a technical solution to allow access to data, without the need to release data out of the HSCIC to external organisations.
- publishes a quarterly register of all releases of identifiable or potentially identifiable data.

During 2014/15, work continued to consolidate strategies, frameworks, and procedures in relation to information governance to improve quality and efficiencies and ensure that information records are:

- held securely and confidentially
- obtained fairly and efficiently
- recorded accurately and reliably
- used effectively and ethically
- shared appropriately and lawfully.

With regard to a summary of other activity in relation to information governance for the year:

- a three-year cyber security programme has been established to instigate a number of projects within HSCIC to provide an enhanced set of information assurance and cyber security capabilities befitting an organisation responsible for the security and protection of personal and patient identifiable data across the health and social care system in England
- an audit function is being established and the organisation is working towards ISO 27001 (information security standard) conformance.
- a new IG Assurance Framework is being developed, which includes significant changes to the IG Toolkit.

***DN. remainder of IG section to be updated April 2014***

- measures have been developed / taken to reduce the burden from data collections on the health and social care system

- each year all staff complete information governance training in line with requirements of the NHS information governance toolkit and more specialist training is undertaken by those staff who are responsible for the management and control of data assets and information
- the HSCIC completed the information governance toolkit. A particular challenge for the HSCIC during 2013/14 has been the secondment of staff in the Data Sharing for Commissioners Regional Offices and ensuring they understand and adhere to the corporate HSCIC information governance policies and processes and contribute to the HSCIC submission of the Information Governance Toolkit
- there have been no personal data incidents in 2013/14 which required reporting to the Information Commissioners Office (ICO). A small number of incidents have been logged and managed internally by the HSCIC. Assessment against ICO guidelines determined these did not require ICO notification due to the minor scale of the incident or that no clinical or sensitive data was included
- the HSCIC is subject to the Data Protection Act 1998 and has filed the appropriate notification with the ICO. During 2013/14, 815 Freedom of Information requests and 46 Subject Access requests were received. There have been four breaches of the timescales for handling a Freedom of Information request and one for handling a Subject Access request. No complaints were made to the ICO by applicants dissatisfied with responses provided to them under the Freedom of Information Act
- as a public information holder, the HSCIC has complied with the cost allocation and charging requirements of HM Treasury and the Office of Public Sector Information. No charges have been made for access to information during 2013/14.
- the HSCIC is committed to the regular review and assurance of all data it handles. In the course of discharging this responsibility, we have discovered in April 2014 a number of NHS organisations that have been submitting data values to the secure Secondary Uses Service (SUS) which do not conform to NHS Data Dictionary Standards. In accordance with good practice and in relation to issues impacting on the use of patient data, we have referred this incident to the Information Commissioner's Office (ICO). We have reminded data providers of their responsibilities and are working with data recipients to support them to delete the affected data. The risk to patient confidentiality has been classified as low by the ICO.

## **Statistical governance**

The HSCIC complies with the Code of Practice for Official Statistics as set by the UK Statistics Authority under the guidance of the Head of Profession for Statistics who oversees

management of two key risks: of breaches of the Code of Practice for Official Statistics and of errors in published figures, both of which are managed through the standard HSCIC risk management processes and escalation routes.

During 2014/15 there were four breaches of the Code of Practice for Official Statistics. One breach related to release practices where a publication was briefly available on the website eight hours before its official publication time. The other three breaches were due to issues with pre-release access: in two instances, the briefing co-ordinators in external organisations mishandled pre-release access material, in one case sending the material to the incorrect NHS contact and in the other, issuing a statement containing embargoed HSCIC figures; in the final breach, a draft document was sent in error to the incorrect contact for review. In accordance with the HSCIC's incident management processes, more rigorous processes have been implemented to prevent recurrence.

The production of some statistics relies on the use of complex models which are deemed to be business critical. In line with the requirements of the Macpherson Report "Review of quality assurance of Government analytical models", the DH framework of quality assurance of business critical models includes two HSCIC statistical models: Summary Hospital-level Mortality Indicator (SHMI) and Better Care, Better Value (BCBV).

### **Public Interest Disclosure**

No Public Interest Disclosures were made to the HSCIC during 2014/15. Our public interest disclosure (whistleblowing) policy was reviewed by National Audit Office in 2013/14 and no significant issues were identified. Nonetheless, we have engaged with *Public Concern at Work* during Q3 with a view to improving our policy and practice in this area, and to embedding a culture in which staff are able to raise concerns in the expectation that they are addressed openly, positively and in a timely manner.

### **Review of effectiveness**

As Accounting Officer, I have responsibility, together with the Board, for reviewing the effectiveness of the system of internal control. My review of 2013/14 has been informed in a number of ways:

- through ARC minutes and papers and its annual report to the Board
- the internal audit plan. I acknowledge this was developed at the start of the year before a full risk assessment had been developed for the organisation, but nevertheless the internal audit team completed a comprehensive range of assessments, and the head of internal audit provided an opinion on the overall arrangements for gaining assurance through the assurance framework and on the controls reviewed as part of the internal audit work. While recognising the challenging circumstances within which the HSCIC operated during the year, the internal audit assurance statement concluded that:  
*There is a generally sound system of internal control, designed to meet the organisation's objectives, and controls are generally being applied consistently. This is supported by our work on key financial and operational processes, which has identified mostly low and medium risk findings.*

*However, our work has also identified some high risk findings in areas which are key to HSCIC's organisational objectives and priorities. These include:*

- *the physical security of buildings and information (including visitor checks, building access controls and tailgating); and*
- *the in-sourcing of the Spine 2 service (including risks relating to the adequacy of project planning and delays in preparing for data migration), although we have noted that a number of management actions were taken prior to the year end to mitigate these risks.*

*Therefore, based on the work we have completed, we believe that there is some risk that objectives in these areas may not be fully achieved. Whilst we are satisfied that these are isolated to specific systems and processes rather than being pervasive to the system of internal control, improvements are required in these areas to enhance the adequacy and / or effectiveness of governance, risk management and control.*

*The basis for forming the opinion is as follows:*

- *we have completed the program of internal audit work for the year ended 2013/14 with the exception of five reviews to be completed in 2014/15. This program of work identified 15 low, 21 medium and 7 high risk findings; and*
- *during the course of our work, we have also become aware of other issues that we believe could have, or have had an impact upon The Health & Social Care Information Centre's system of internal control. These matters were raised within separate assurance related reviews outside of the agreed programme of internal audit work, both of which identified high risk findings as follows:*
  - *our work on Data Services for Commissioners Regional Offices (DSCROs) identified a range of findings relating to information governance at the DCSROs; and*
  - *our review of BT SUS Security identified a high risk finding relating to the lack of systematic audit logging or monitoring within the SUS environment.*

*We also note the following limitation of our opinion:*

- *a detailed review of risk management was not performed and was instead deferred into the 2014/15 year at management's request. As a result, our work on risk management was limited to a high level review and commentary on the developing framework only, and we are not able to form a definitive conclusion on the effectiveness of risk management processes during 2013/14; and*
- *is based solely on the annual internal audit activity of 263 days for 2013/14, and on our assessment of whether the controls in place support the achievement of management's objectives as set out in our Annual Internal Audit Risk Assessment and Plan and individual assignment reports.*

- following individual audit reports, action plans were put in place to address recommendations with progress reviewed by the ARC on a regular basis
- senior managers within the organisation who had responsibility for the development and maintenance of the system of internal control provided the former interim Chief Executive with assurances
- through clear performance management arrangements in place with executive directors and senior managers
- the assurance framework itself provided evidence on the effectiveness of controls that managed the risks to the organisation
- by the findings of the National Audit Office as the organisation's external auditors

- by review of and accepting a report from Alan Perkins (Accounting Officer to 31 March 2014) dated 31 March 2014 confirming that appropriate governance was in place until this date.

I have been advised on the effectiveness of the system of internal control by the Board and the ARC of the HSCIC and am accordingly aware of any significant issues that have been raised.

### **Significant Internal Control Issues**

I recognise that during the year certain control issues have arisen that need addressing as a priority in 2014/15. The key concern was in relation to the accounting for non-current assets an area also raised by the NAO who have rightly drawn them to my attention.

We started the year with a very incomplete non-current asset register and processes that were substantially inadequate for providing an appropriate level of control. Although we have made sufficient progress on our record keeping and processes to give me adequate assurance for our 2013/14 Accounts, we need to invest further to make the necessary improvements in the year ahead.

The starting position was in part due to the granularity of the information provided to the HSCIC when it was formed. We have also had to assimilate IT equipment from other organisations, and consolidate the infrastructure across a number of external data centres partly as a means of increasing efficiency, but also improving the physical security and resilience of the systems and the confidentiality of data contained on them. The particular issues included the following:

- the identification of assets belonging to the HSCIC in the DH ledger was incomplete. The HSCIC inherited only a small fraction of the assets formally held by CfH contained on the DH ledger, and although the HSCIC manages the delivery of the continuing former CfH programmes, we are not involved in their management or record keeping
- the underlying accounting records at the start of the financial year in some important cases fell well short of the standard needed, and although we have made significant improvements to the records we still have more work to do
- the impact of inadequate records was compounded because we found it difficult to prove the existence of some of the assets transferred, particularly physical IT equipment where assets were componentised and located in external data centres
- the “equipment list” maintained by IT for internal asset management purposes was not complete or reconciled to the accounting records and thus was not sufficiently robust for financial reconciliation purposes
- there was an insufficiently robust process for determining the correct accounting treatment for complex software developments and licence arrangements including the classification between non-current asset categories and adherence with the requirements of the relevant accounting standards
- reviewing the assets transferred from the various organisations which employed different capitalisation and depreciation policies.

Most of these issues were highlighted early in the audit planning cycle, and my finance team assigned additional resources to complete remedial work to improve our records and put in place improved control processes. I am satisfied that we now have adequate control, but given the value and the importance of the IT assets generally to the organisation, I am firmly

committed to putting our asset management onto a much more robust footing. Our provisional plan of action includes the following:

- undertake a full asset verification exercise in the autumn of 2014
- seek to build a single asset management database that serves a multitude of purposes for the organisation
- undertake a review of our asset life policy
- establish closer working with between the finance, IT and procurement team, to ensure all teams are using an agreed and robust process, transactions are undertaken based on robust technical advice and all staff have clarity over roles and responsibilities.

My finance and IT teams are still working on the details, but I will fully support all and every action they need to take to provide the highest possible assurance that we have a robust and effective approach to managing our non-current assets. I expect this to include the appointment of a dedicated accountant, investment in the development of a database, and substantial work by our finance, IT and procurement teams working collaboratively.

Other concerns include:

- an urgent need for a comprehensive internal assurance map which will provide the Board and DH with systematic assurance that risk management is internal controls are in place across the organisation
- aspects of resilience to social engineering and BT SUS security. These, along with wider Government concerns over cyber security, have been a significant driver for an overhaul of information and physical security arrangements within the HSCIC which will continue under the oversight of the new Information Assurance and Cyber Security sub-Committee of the Board
- the controls surrounding data released by the NHS IC, one of our predecessor organisations. From April 2005 to March 2013, its role had been to collect and manage health records data, including sharing it with third parties under data sharing agreements which restricted its use. The Board commissioned an independent review by PricewaterhouseCoopers which was published in June 2014. PwC identified lapses in the strict arrangements that were supposed to be in place to ensure that people's personal data would never be used improperly, although the failings in terms of the processes, control and overarching governance were not systemic. The HSCIC is committed to implementing all the recommendations arising from the review.

I fully accept and welcome these observations on our controls.

Wherever practical mitigation measures have also been put in place against externally generated risks from across the wider health and social care system over which HSCIC has no direct control and which are for DH to consider. Finally, assurance advice has been sought from internal audit on the information governance processes and framework controls in place at Data Services for Commissioners Regional Offices (DSCROs). Although not conducted as a formal audit their advice through a series of phased reviews has provided a series of recommendations to strengthen the controls which are presently being considered.

I believe that the HSCIC started the year with governance and internal control arrangements which were less than effective but which it has taken significant steps to strengthen. But much remains to be done and this will continue to be addressed as a priority during 2014/15.

**Andy Williams**  
**Accounting Officer**  
**XX June 2015**

## Annex

### HSCIC Board 2014/15

Membership	Meetings Attended	Role
<p><b>Board</b>  <i>Non-executive directors:</i></p> <p>K Manning (Chair)</p> <p>Sir I Andrews (Senior Independent Director)            Sir N Partridge (Vice Chair)            Sir J Chisholm            Prof. M Goddard            J Ormondroyd - until 19/10/2014            Dr S Blackburn – from 15/09/2014</p> <p><i>Executive directors:</i></p> <p>A Williams (CEO)            R Allsop            R Shaw (Senior Information Risk Owner (SIRO))            C Vincent            M Jones – until 06/03/2015</p> <p><i>Other directors:</i></p> <p>T Denwood            J Hawkins            P Counter – from 16/06/2014            I Hunt – from 06/10/2014            Prof. M Severs (Caldicott Guardian and Lead Clinician)</p>		<p>Board members have corporate responsibility for ensuring that the HSCIC complies with any statutory or administrative requirements for the use of public funds. The powers retained by and the responsibilities of the Board include:</p> <ul style="list-style-type: none"> <li>▪ Agreeing the vision and values, culture and strategy of the HSCIC within the policy and resources framework agreed with the Department of Health sponsor</li> <li>▪ Agreeing appropriate governance and internal assurance controls</li> <li>▪ Approving business strategy, business plans, key financial and performance targets and the annual accounts</li> <li>▪ Ensuring sound financial management and good value for money</li> <li>▪ Ensuring controls are in place to manage financial and performance risks, including ensuring that the HSCIC has the capability to deliver its strategic objectives</li> <li>▪ Using information appropriately to drive improvements</li> <li>▪ Supporting the Executive Management Team and holding it to account</li> <li>▪ Ensuring the Board is able to account to Parliament and the public for how it discharges its functions</li> <li>▪ Ensuring that the HSCIC complies with any duties imposed on public bodies by statute, including without limitation obligations under health and safety legislation, the Human Rights Act 1998, the Disability Discrimination Act 2005, the Race Relations (Amendment) Act 2000, the Data Protection Act 1998, the Freedom of Information Act 2000 and the Equality Act 2010</li> <li>▪ Ensuring that the HSCIC has specific responsibility for sustainable development and operates within the framework of the Department of Health’s environmental policies.</li> <li>▪ Approving recommendations of Board committees</li> <li>▪ Approving income and expenditure as defined</li> </ul>

	<p>in the HSCIC Levels of Delegated Authority document</p> <p>Further details including the conduct of meetings are contained in the HSCIC Corporate Governance Manual incorporating the Standing Orders and Standing Financial Instructions, and other governance documents.</p> <p>The statutory Board meetings comprised a public session, where members of the public were able to attend, with all minutes and papers made available on the HSCIC website. In addition, from time to time, the Board needed to consider commercial or confidential items that could not be discussed in public. In that event a private session was held without any observers.</p>
--	--

#### HSCIC Assurance and Risk Committee 2013/14

Membership	Meetings Attended	Role
<p><i>Non-executive directors:</i></p> <p>Dr S Blackburn (Chair) – from Nov 2014            Sir I Andrews (interim Chair - until Oct 2014)            Sir N Partridge            Sir J Chisholm            J Ormondroyd – until Oct 2014            Prof. M Goddard – from Nov 2014</p> <p><i>Executive directors - in attendance:</i>            A Williams            C Vincent            R Shaw            R Allsop – from Nov 2014            M Jones – until Oct 2014</p> <p><i>Other directors in attendance:</i>            J Hawkins – from Nov 2014            In addition, representatives of both the internal and external auditors attend the meetings.</p>		<p>The Board delegated full responsibility to the Assurance and Risk Committee to:</p> <ul style="list-style-type: none"> <li>▪ Investigating any activity within the terms of reference. The Committee was authorised to seek any information that it requires from any employee and all employees are directed to cooperate with any request made by the Assurance and Risk Committee</li> <li>▪ Obtaining outside legal or independent professional advice, at the HSCIC's expense, and to secure the attendance of external specialists with relevant experience and expertise if it considers this necessary</li> </ul> <p>The committee was charged with providing assurance and making recommendations to the Board on:</p> <ul style="list-style-type: none"> <li>▪ The operational effectiveness of policies and procedures</li> <li>▪ The policies and procedures for all work related to fraud, corruption and whistleblowing, including the appointment of a Local Counter Fraud Specialist and to enable the Local Counter Fraud Specialist to attend Assurance and Risk Committee meetings when required.</li> <li>▪ An effective internal audit function established by management that meets mandatory internal audit standards and provides appropriate</li> </ul>

		<p>independent assurance to the Chief Executive and Board</p> <ul style="list-style-type: none"><li>▪ The effectiveness of the system of integrated governance, risk management and internal control including information governance, security and data quality risks</li><li>▪ The accounting policies, the accounts and the annual report of the organisation</li><li>▪ Planned audit activity and results of both internal and external audit reports</li><li>▪ Any required changes to key corporate governance documents (for example the Corporate Governance Manual, standing orders, standing financial instructions and the scheme of delegation)</li></ul>
--	--	---

## HSCIC Remuneration Committee 2014/15

Membership	Meetings Attended	Role
<p><i>Non-executive directors:</i> K Manning (Chair)</p> <p>Sir N Partridge Prof. M Goddard J Ormondroyd - until Oct 2014</p> <p><i>Executive directors – in attendance:</i> A Williams R Allsop</p>		<p>The Board delegated full responsibility to the Remuneration Committee to:</p> <ul style="list-style-type: none"> <li>▪ Make recommendations to the Department of Health (DH) on the level of the remuneration packages of the CEO and other executive directors within the provisions of the Pay Framework for Very Senior Managers (VSMs) or successor arrangements</li> <li>▪ Determine pay arrangements for medical and other staff groups who are not subject to Agenda for Change (AfC), VSM or the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE) protected terms and conditions of employment</li> <li>▪ Maintain an overview of senior non-medical staff pay (currently defined as over £100,000 per annum, including any award of Performance Related Pay) to ensure that pay remains consistent with public pay policy</li> <li>▪ Approve the level of any annual performance related pay awards to HSCIC staff on ex-Civil Service terms and conditions</li> <li>▪ Approve the annual performance objectives and targets of executive Directors</li> <li>▪ Monitor and evaluate the performance of VSMs and make recommendations to DH) on any proposed annual performance pay awards within the total of VSM pay bill which may be used for performance related pay (as set annually by DH, taking account of the recommendations of the Senior Salaries Review Body)</li> <li>▪ Ensure that pay arrangements are appropriate in terms of Equal Pay requirements.</li> <li>▪ Consider and approve redundancy payments and other (often TUPE related) exceptional matters</li> <li>▪ Ensure that all matters relating to pay and conditions that require approval from the Department of Health Remuneration Committee or other external authority are submitted for approval and that the decisions of those bodies are appropriately implemented.</li> </ul>

## HSCIC Information Assurance and Cyber Security Committee (IACSC) 2014/15

The inaugural meeting of the HSCIC IACSC was held on 13 May 2014.

Membership	Meetings Attended	Role
<p><i>Non-Executive Directors:</i>            Sir I Andrews (Chair)            Sir N Partridge            J Ormondroyd – until Oct 2014            Prof. M Goddard – from Nov 2014</p> <p><i>Executive Directors – in attendance:</i>            A Williams            R Shaw            R Allsop</p> <p><i>Other directors in attendance:</i>            Peter Counter – from July 2014            Prof. M Severs</p> <p>In addition, representatives from cross government organisations attend the meetings.</p>		<p>The Board delegated full responsibility to the Information Assurance and Cyber Security Committee to:</p> <ul style="list-style-type: none"> <li>▪ Investigate any activity within the terms of reference. It was authorised to seek any information that it requires from any employee and all employees are directed to cooperate with any request made by the Information Assurance and Cyber Security Committee</li> <li>▪ Obtain outside legal or independent professional advice, at the HSCIC's expense, and to secure the attendance of outsiders with relevant experience and expertise if it considers this necessary.</li> <li>▪ Ensure that there is an effective Information Assurance function that meets recognised industry and Government standards and provides appropriate independent assurance to the Chief Executive and Board.</li> <li>▪ Review the work and findings of the Cyber Security Programme and take account of the implications and management responses to their work.</li> <li>▪ Review the findings of other significant assurance functions, both internal and external to the organisation, and consider the implications to the governance of the organisation.</li> </ul>