

# HSCIC Information Assurance Brief – Interim Cyber Security Review

**The Importance of Information Assurance and Cyber  
Security for Health and Social Care**

**October 2013**

## Purpose

1. To provide information about the HSCIC approach to **Information Assurance and Cyber Security** and a high level view of the results of the **Interim Cyber Security Review**.

## Background

2. Information Assurance is the process of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information Assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of data. It uses physical, technical and administrative controls to accomplish these tasks.
3. Cyber Security covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorised access, change or destruction. Cyber Security has recently crystallised to look at “sophisticated, motivated, well-funded and well equipped” threats to systems, services and organisations. In this regard, Cyber Security is considered a crucial component of a mature over-arching Information Assurance approach.
4. As an information services organisation, it is critical to the HSCIC’s ability to deliver programmes and services and to our reputation that we have a robust approach to Information Assurance and that we are perceived publicly as having such a robust approach to Information Assurance and Cyber Security across the Health and Social Care system.
5. Cyber Security is recognised as a top level Tier 1 risk by Government and is quickly establishing itself as one of the key risks which executive boards are now considering as core to their business strategy and management. The Health and Social Care System, given the size and variety of organisations it is involved with, has a large threat profile, but a lower likelihood risk of compromise due to not being the target motivations of the most serious Cyber Threats.

## A view from Sir Ian Andrews, Non-Executive Director, HSCIC

6. What sets the HSCIC apart is that it is the only one of the new statutory Arm’s Length Bodies created by the Health and Social Care Act that is empowered to collect and hold patient confidential information across the health and social care system. Vital to our credibility is that patients, service users and health and social care professionals trust us, together with our systems and processes, to ensure that the data is effectively safeguarded and available to those who legitimately need access to it, while protected from inappropriate exploitation.
7. In a world that is ever more reliant on digital and mobile technology, this poses many very real challenges. Our ambition must be to be recognised as the best provider of objective, dispassionate and authoritative data – including clinical management and performance information – to support the delivery of health and social care in England. We must set the standard for others to aspire to in the assurance and security of the information we collect, hold and publish.
8. The Board is determined to ensure that the already high levels of assurance inherited from the various bodies that came together to form the Centre are built upon and continuously refined to ensure that they are at all times fit for purpose. This review, and the action plan which flows from it, are vital to this process.

## HSCIC Interim Cyber Security Review

9. The HSCIC Board has instructed the Information Assurance Directorate to undertake a high level review of Cyber Security across the organisation. This has involved workshops, document reviews and one to one sessions. The review was conducted to tight timelines and the Infrastructure Security Team would like to thank all our contributors for their time and expertise.
10. The findings of the review have highlighted that through the merging of the original NHS CFH and NHS Information Centre organisations, **the opportunities and expertise which are now available provide the means and resources to meet the challenge of securely protecting** an ever changing Health and Social Care system. Through the findings of the review, the HSCIC Board and Executive can direct and focus the efforts of our expertise to those areas and services which maintain our continued assurances. Given our legal role as safe haven for personal and confidential information, we need to stand as an exemplar organisation for the management of sensitive and confidential information.
11. As the HSCIC transforms and meets these challenges, there are new threats and risks which must be assessed and mitigated. This requires strong leadership, dedication to excellence and the continued vigilance of the people and processes upon which our assurance relies. The review has recommended that the organisation should take a system level view of the risks and threats presented by Cyber Security. With an **organisational wide approach to risk management**, Cyber Security and its companion areas can be managed in a collaborative manner so that the reporting, management and resolution of risks is handled in a structured and governed way.
12. The HSCIC must also examine the processes and procedures which govern our approach to designing, developing, deploying and managing the systems and services we rely upon as an organisation and those we deliver to the wider Health and Social Care system. Through **continuous assessment and consequent evolution** of our approaches, the HSCIC can build upon its existing reputation as the champion of information services, which support the delivery of world class Health and Social Care to patients.
13. The **HSCIC has a rich and embedded culture of security and information governance** from the legacy of the organisations out of which it is formed. Through mandated contractual requirements to legally binding agreements and contracts for data sharing, the HSCIC is well placed to continue to deliver the world class services and system to support the wider system. This reputation is further enhanced through continued working and collaboration with wider Government programmes related to Cyber Security and Information Assurance, which systems and solutions need to interoperate with.
14. The findings of the review have recommended that the Board endorse and sponsor the initiation of a number of work streams which will deliver improvements and management of change across the organisation. The streams will also provide the mechanisms by which the **existing excellence and good practice which the HSCIC implements is shared across the wider Health and Social Care system**, and out further across our Public Sector and Government partners.
15. Through the implementation of the recommendations of the review, and through the commitment of the Board and Executive, the HSCIC will continue to demonstrate its **central role in the provision of safe, secure and legally compliant management of confidential and sensitive information**. This information is crucial to providing benefits to the whole Health and Social Care system and the patients it serves.

Clare Sanderson, Director of Information Assurance