Directorate / Programme	**Data Dissemination Services**	Project	**Data Sharing Audits**
		Status	**Approved**
Director	**Terry Hill**	Version	**2.0**
Owner	**Rob Shaw**	Version issue date	**21/04/2016**

HSCIC Audit of Data Sharing Activities:

University of Nottingham

Contents

Executive Summary

This document records the key findings of a Data Sharing Audit[1] at the Division of Primary Care of the University of Nottingham, on 28th and 29th January 2016 against the requirements of the Health and Social Care Information Centre (HSCIC) in relation to data sharing agreement NIC-376367-M5V9H covering the supply of the full dataset for Hospital Episode Statistics (HES) data on a quarterly basis.

This audit used an approved and mature methodology based on ISO standard 19011: 2011 (Guidelines for auditing management systems) and follows the same format for all audits of data sharing agreements conducted by the HSCIC.

In total, three major non-conformities, seven minor non-conformities and two observations were raised[2] based on the findings of the onsite visit:

- The University of Nottingham used an IT Contractor as a data processor with full access to the system including all databases. There was no separation of duties for access to the HES data and the salt. Furthermore, whilst controls were in place, the Audit Team found that not all of the expected controls based on the ICO Anonymisation: managing data protection risk - Code of Practice 2012 were in place. The University of Nottingham and the HSCIC have been reviewing and improving the controls in place over the lifetime of the data sharing arrangements. As an additional improvement, the University of Nottingham has transferred control of the salt to the data controllers. This means that the University of Nottingham no longer holds de-identified personal data. (Major)
- No evidence was presented to show that the HES data are treated as de-identified personal data or had been assessed against the eight data protection principles. Furthermore the University's data protection registration entry did not include subjects of healthcare as a type of data subject. HES data that was not related to the population being studied was retained instead of being permanently deleted. (Major)
- There was no documented evidence that a local risk register existed and there was no review of risks between April 2011 and December 2015. (Major)
- There were differences in the System Level Security Policy and the Information Security Policy (and other University processes).This includes reporting of system breach to IT Services, using a WEEE approved contractor for IT asset disposal and ISO 27001 statement. The system is maintained by the IT Contractor and is not centrally controlled by IT Services, which is the basis of some of the controls in the Information Security Policy. The System Level Security Policy had not been reviewed and approved by University of Nottingham IT Services. (Minor)

[1] An audit is defined by ISO 9000:2014 as a *systematic and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the **audit criteria** are fulfilled*

[2] Definitions found **in** Section 1.4

- There was no documented assessment confirming that non University laptops are used to carry out the processing of the data on the server had been assessed against the University of Nottingham's Desktop, Laptop and Mobile Security Policy to ensure they met configuration requirements. There was no reference in the Data Sharing Agreement or System Level Security Policy that laptops which were not University property would be used to access the HES data. Furthermore, the IT asset register does not include details of these laptops. (Minor)
- The Audit Team found that there was no technical control enforcing minimum password length on two servers and the level of encryption one of the server holding the salt was 128bit, instead of 256 bit AES. The University's Encryption Policy recommends 256 bit AES encryption for long term security. The University of Nottingham Password Policy requires that the password is a minimum of seven characters and control mechanism enabled. (Minor)
- The secondary firewall between the University of Nottingham network and the servers where the HES data is stored was last patched in 2006, had reached end of life in December 2015 and is no longer supported (including security updates) by the manufacturer. In the absence of a network equipment patching policy, the Server Security policy requires that security patches must be installed on the system within seven days and the device should not be designated as 'end of life'. It should be noted that this is a secondary firewall behind the main University of Nottingham firewall and has been subjected to penetration testing. (Minor)
- An external penetration test of the salt key server and the network for the servers holding HES data was commissioned and completed in January 2016. The independent report had been separated into two parts. The second part (covering the HES data) was made available to the Audit Team after the onsite visit and the University stated the first part of the report (covering the salt key server) would only be made available after the recommendations had been implemented. The scale of these recommendations was not shared with the Audit Team. The Data Sharing Framework Contract clauses 7.3 and 7.4 require the data recipient provides information requested during an audit so that the HSCIC can verify compliance with the contract and agreement. (Minor)
- The process documented in the System Level Security Policy on data destruction and hardware disposal is not consistent with the University of Nottingham agreement in that assets were not destroyed through a University of Nottingham approved Waste Electrical and Electronic Equipment (WEEE) contractor and suitable confirmation provided. (Minor)
- The University's Asset Management Policy requires that information assets are classified based on the sensitivity of the information they contain and states risk assessments should be carried out on the assets. This classification and assessment had not been carried out on the HES information assets. Furthermore, there was no evidence to support that the Senior Information Risk Officer (SIRO) had been made aware of the HES information assets or details about the risk assessments. (Minor)

- A reference to the HSCIC guidance for reporting, managing and investigating information governance and cyber security serious incidents is added to the University guidance to ensure that appropriate reporting is initiated in the event of certain incidents occurring. (Observation)
- A copy of the HES backup tape is taken off site and stored in a safe at a private, non-university location. Whilst this practice does not breaching the University of Nottingham's Backup Policy, there needs to be clear guidance on the offsite storage of backup tapes. This is also not fully explained in the System Level Security Policy. (Observation)

Areas of Good Practice

- The University are producing clear tangible outputs which show direct benefits to health and social care through the analysis of the HES data linked with general practice data.
- The servers holding the HES data and the backup tapes used 256 bit AES encryption.
- An IT Contractor is conducting monthly administration checks on the servers holding HSCIC data and suitable evidence is being maintained in the system administration log.
- External risk assessments were commissioned and completed in March 2011 and January 2016.
- A penetration test of the infrastructure holding the HES data did not identify any concerns.

The University of Nottingham has reviewed this report. The University will establish a corrective action plan to address each finding. These plans will be validated at a follow-up meeting with the University of Nottingham to confirm the proposed actions satisfactorily address the nonconformities raised.

In summary, it is the Audit Team's opinion that at the time of the audit and based on evidence presented on the day, there was risk of inappropriate exposure and / or access to data provided by HSCIC to the University of Nottingham under the terms and conditions of data sharing agreement NIC-376367-M5V9H and associated data sharing framework contract signed by both parties.

1 About this Document

1.1 Introduction

The Health and Social Care Act 2012 contains a provision that health and social care bodies and those providing functions related to the provision of public health services or adult social care in England handle confidential information[3] appropriately.

The Review of Data Releases by the NHS Information Centre[4] produced by HSCIC Non-Executive Director Sir Nick Partridge recommended that the HSCIC should implement a robust audit function that will enable ongoing scrutiny of how data are being used, stored and deleted by those receiving it.

In August 2014, the HSCIC commenced a programme of external audits with organisations with which it holds data sharing agreements. The established audit approach and methodology is using feedback received from the auditees to further improve our own audit function and our internal processes for data dissemination to ensure they remain relevant and well managed.

Audit evidence was evaluated against a set of criteria drawn from the HSCIC's Code of Practice on Confidential Information[5], data sharing framework contract, data sharing agreements signed by the relevant contractual parties and the international standard for Information Security, ISO 27001:2013.

1.2 Background

The Division of Primary Care of the University of Nottingham is linking HES data to general practice data. The servers holding HES data are located at the University of Nottingham and are subject to the University's security assurance and data protection registration.

The University requires as a pre-requisite for linking the HES data to other sources of data that the HSCIC uses the OpenPseudonymiser. This allows the HSCIC to pseudonymise the NHS number at source using a salt[6] shared with the other providers of data.

[3] Confidential information is defined by the Code of Practice on Confidential Information as data which:

- Identifies any person
- Allows the identity of anyone to be discovered, including pseudonymised information
- Is held under a duty of confidence

[4] www.hscic.gov.uk/datareview

[5] www.hscic.gov.uk/cop

[6] random data used in the one-way hash algorithm to convert the NHS number into a pseudonymised NHS number to enable linkage with other sources of data

The methodology was jointly proposed to the Ethics and Confidentiality Committee by the NHS Information Centre and the University of Nottingham in 2011 who confirmed that the University did not require support under the Control of Patient Information Regulations to process and link pseudonymised HES data for research purposes adopting that methodology.

The security of the salt is critical in order to support the University of Nottingham data sharing agreement for patient level pseudonymised data.

1.3 Purpose

This report provides an evaluation of how the University of Nottingham conforms to the requirements of the data sharing agreement NIC-376367-M5V9H covering the supply of patient-level pseudonymised and non-sensitive datasets and the associated data sharing framework contract.

It also considers whether the University of Nottingham conforms to its own and the policies and procedures. This report provides a summary of the key findings.

1.4 Nonconformities and Observations

Where a requirement of either the data sharing agreement or the audit criteria was not fulfilled, it is classified as a Major Nonconformity or Minor Nonconformity. Potential deficiencies or areas for improvement are classed as Observations.

1.4.1 Major Nonconformity

The finding of any of the following would constitute a major nonconformity:

- the absence of a required process or a procedure
- the total breakdown of the implementation of a process or procedure
- the execution of an activity which could lead to an undesirable situation
- significant loss of management control
- a number of Minor Nonconformities against the same requirement or clause which taken together are, in the Audit Team's considered opinion, suggestive of a significant risk.

1.4.2 Minor Nonconformity

The finding of any of the following would constitute a minor nonconformity:

- an activity or practice that is an isolated deviation from a process or procedure and in the Audit Team's considered opinion is without serious risk
- a weakness in the implemented management system which has neither significantly affected the capability of the management system or put the delivery of products or services at risk
- an activity or practice that is ineffective but not likely to be associated with a significant risk

1.4.3 Observation

An observation is a situation where a requirement is not being breached but a possible improvement or deficiency has been identified by the Audit Team.

1.5 Audience

This document has been written for the HSCIC Director of Data Dissemination Services. A copy will be made available to the HSCIC Community of Audit Practitioners, Assurance and Risk Committee and the Information Assurance and Cyber Security Committee for governance purposes. The report will be published in a public forum.

1.6 Scope

An audit notification letter was sent to the University of Nottingham on the 5th January 2016. The audit considered the fitness for purpose of the main processes of data handling at the University of Nottingham along with its associated documentation.

Fundamentally, the audit sought to elicit whether:

- the University of Nottingham is adhering to the standards and principles of the data sharing framework contract, data sharing agreements and audit criteria
- data handling activities within the organisation pose any risk to patient confidentiality or HSCIC.

1.7 Audit Team

The Audit Team was comprised of a senior certified ISO 9001:2008 (Quality management systems) auditor and a Certified Information System Auditor (CISA) auditor.

The audit was conducted in accordance with ISO 19011:2011 (Guidelines for auditing management systems).

2 Audit Findings

This section presents the key findings arising from the audit.

2.1 Operational Planning and Control

The University's application for HES data was on the basis that the data are effectively pseudonymised with safeguards to limit access in line with Chapter 7 of Information Commissioner's Office Anonymisation: managing data protection risk code of practice. The Audit Team found evidence and controls concerning limitation to agreed purposes, management controls over the ability to bring other data into the data processing environment and limitation of use to projects through the adoption by the University of Nottingham of the Good Clinical Practice Guidelines.

The University of Nottingham had access to the components that could be used to potentially derive NHS numbers. NHS numbers are described in the University of Nottingham "Clinical Research Governance Policy – Confidentiality and Personal Data" as identifiable data. At the time of the audit, the University of Nottingham was therefore in control of de-identified personal data[7] that was sensitive data and confidential information.

An IT Contractor is employed to provide IT support including IT security, database administration and off site hardware disposal. The contractor had full access to the systems including the databases and the salt. There was no separation of duties for access to the HES data and the salt. The Audit Team reviewed the University's contract (with amendments) with the IT Contractor and found no reference to database administration of the HES data or IT disposal (see section 2.4). The Audit Team did not find all of the expected controls based on the ICO Anonymisation: managing data protection risk - Code of Practice 2012.

The System Level Security Policy provides assurance that good information governance practices are being maintained as a part of the Data Sharing Framework Contract. This assurance control was reviewed by the HSCIC prior to the data sharing agreement.

The University of Nottingham provided a copy of the advice it received in 2011 from the Ethics and Confidentiality Committee of the National Information Governance Board. The advice stated that support under the Health Service (Control of Patient Information) Regulations 2002 would not be required.

[7] data which relate to a living individual who can be identified:

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Audit Team did not see any evidence that the HES data are treated as de-identified personal data or had been assessed against the eight data protection principles. Furthermore, the University's data protection registration entry did not include subjects of healthcare as a type of data subject.

Although a full extract of the HES data set is provided to the University of Nottingham, only a subset of the data is linked to primary care data. The Audit Team noted the data concerning patients who are registered with GP practices not participating in the research and therefore not linked was nevertheless retained instead of being permanently deleted.

There are a number of policies included in the University of Nottingham Information Security Policy including Anti-Virus Policy, Encryption Policy, Asset Management Policy, Password Policy and Server Security Policy.

The System Level Security Policy outlines the IT controls for the HES data. The policy had been written by the Project Lead and was updated on the 5th January 2016. However, the policy had no version control (although this was provided on the day) and there were differences in the System Level Security Policy and the University guidance including the Information Security (IS) Policy. This includes reporting of system breach to IT Services, (IS Policy -section 1.2.3) and using a WEEE approved contractor for IT asset disposal. The system is maintained by the IT Contractor and is not centrally controlled by IT Services, which is the basis of some of the controls in the Information Security Policy.

The Audit Team noted that an internal audit report in 2011 made a recommendation that '*the statement that the University's Information Security Policy adheres to ISO 27001 should be amended to a more factually correct statement'*. This has not been actioned. The System Level Security Policy had not been reviewed, assessed and approved by the University of Nottingham IT Services to ensure it was compatible with corporate policies including the Information Security Policy**.**

Data are disclosed or published by the University of Nottingham in anonymised tabular form with small number suppression. Contractual requirements are in place to limit linkage to that permitted in the data sharing agreement. The University's data protection breach document sets out the steps to be followed after a data breach. The Audit Team suggested that a reference to the HSCIC guidance for reporting, managing and investigating information governance and cyber security serious incidents is added to ensure that appropriate reporting is initiated in the event of certain incidents occurring. The document also refers to a hyperlink on the ICO website, which is no longer working.

Staff are required to undertake information governance training. The training records provided showed that both the Project Lead and IT Contractor had completed the training in January 2016.

Conclusion: A number of major issues were identified in respect of how the University viewed and handled HES data and the use of an external contractor.

The University of Nottingham and the HSCIC have been reviewing and improving the controls in place over the lifetime of the data sharing arrangements. As an additional improvement, the University of Nottingham has transferred control of the salt to the data controllers. This means that the University of Nottingham no longer holds de-identified personal data.

2.2 Access Controls

Two non-University laptops are used to connect to the University network and access the server where the HES data are processed. It was noted that no processing of the HES data takes place on the laptop; however it was still possible to transfer data from the backup HES server onto the laptops. At the time of the audit, there was no documented assessment confirming that the laptops had been assessed against the University of Nottingham Desktop, Laptop and Mobile Security Policy to ensure they met configuration requirements. There was no reference in the data sharing agreement or System Level Security Policy that non University laptops would be used to access the HES data. Furthermore, whilst the research team has an IT asset register, it does not include details of these laptops that are required to carry out the processing of the data on the server.

The servers are housed in an office that has been converted into a server room. The room is kept locked and access to the room is restricted to named individuals. There are a number of environmental and physical access controls in place including CCTV. In March 2011, an external risk assessment was commissioned by the University to assess the controls in place. This was reviewed in January 2016.

The server room includes two servers that hold HES data. The HES data on the primary server are backed up to tape and then restored onto the second server. At the time of the audit, there was another server in the room on a separate network that held the salt.

The IT Contractor undertakes a number of system administration checks on a monthly basis, which are logged and reviewed by the Project Lead. The Audit Team reviewed the server configuration security for the two servers holding the HES data and the key server holding the salt. Access to the servers holding the HES data have been restricted to two high privileged accounts, which have been assigned to the IT Contractor and the Project Lead. The IT Contractor also had a privileged account on the key server. There was an audit trail for all the privileged accounts.

The Audit Team found that a number of controls for the servers were in place including restriction on assets that can connect to the server, patch management, data on the server was encrypted and logging and monitoring of accounts including an email alert system. The University of Nottingham Password Policy requires that the password is a minimum of seven characters and control mechanism enabled. The Audit Team found that there was no technical control enforcing minimum password length on the two servers and the level of encryption of the server holding the salt was 128bit, instead of 256 bit AES. The University's Encryption Policy recommends 256 bit AES encryption for long term security.

The Audit Team noted that the salt key server had been rebuilt in January 2016 and prior audit logs were not available.

Systems are in place to back up the HES data onto tape with a number of checks carried out to ensure that the backups have been completed successfully. The backup tapes are encrypted using 256 bit AES. The data are backed up onto two tapes. The first tape is kept in a secure cage in the server room. The second tape is taken off site. The Audit Team established that the second tape was taken to and stored at a private, non-university location. The Audit Team noted that this is not fully explained in the System Level Security. Whilst this practice was not breaching University of Nottingham's Backup Policy, there needs to be clear guidance on offsite storage of backup tapes and assessment. The Project Lead also had access to the encryption key in exceptional circumstances.

Conclusion: Controls have been established to restrict access to the HES data. However instances were identified where University policy had not been met. The suitability of the approach to the storage of the backup tapes was questioned by the Audit Team and improvements to University policy are sought.

2.3 Information Transfer

The HES dataset is made available on the HSCIC Secure Electronic File Transfer (SEFT) portal. The Project Lead downloads the zip file and it is saved directly onto a dedicated server. The file is unzipped and the datasets imported into the database followed by data quality checks. The HES data are processed on the server by the Project Lead. The HES data are linked to primary care data and other data which the University of Nottingham obtains from other sources using the same pseudonyms.

Researchers from other bodies are not permitted access to the patient level data. Access to the linked database is restricted. Access would only be granted to University of Nottingham research staff after meeting specific criteria and approval by the division's Advisory Board. The Audit Team was informed that no researchers had access to the linked database at the time of the audit.

The secondary firewall between the University of Nottingham network and the servers where the HES data are stored was last patched in 2006, reached end of life in December 2015 and is no longer supported (including security updates) by the manufacturer. In the absence of a network equipment patching policy, the Audit Team referred to the University's Server Security policy which requires that security patches must be installed on the system within seven days and the device should not be designated as 'end of life'. It should be noted that this is a secondary firewall behind the main University of Nottingham firewall and has been subjected to penetration testing.

An external penetration test of the infrastructure holding the salt and the network for the servers holding HES data was commissioned and completed in January 2016. The independent report was not made available to the Audit Team during the onsite visit. The Audit Team were advised that the report had been separated into two parts. The second part covering the HES data was made available to the Audit Team after the onsite visit. This part did not identify any concerns. The University stated that the first part of the report, which looked at the salt key server, would only be made available after the recommendations had been implemented. The scale of these recommendations was not shared with the Audit Team. The Data Sharing Framework Contract clauses 7.3 and 7.4 require the data recipient to provide information requested during an audit in order to verify its compliance with the contract and agreement. No evidence was provided that indicated that a penetration test had been commissioned prior to January 2016. The Audit Team noted that the servers are linked to the Internet for patching through multiple level firewalls.

A number of papers have been written by the Project Lead, which showed direct benefit to the health and social care system. The results from the research undertaken have resulted in new knowledge and understanding regarding disease epidemiology, health inequalities, drug safety, methods of identifying patients at high risk of serious illnesses.

The research work has also been used to inform national policy.

Conclusion: The University had commissioned an independent penetration test. One part of the report covering the HES data did not identify any concerns. The second part would only be made available after identified vulnerabilities had been resolved.

2.4 Disposal of Data

The Audit Team was provided with an extract of the University of Nottingham agreement with an approved IT hardware disposal company. The extract covers Reuse, Recycling and Disposals and outlines that all Hard Disc Drives (HDD) should be wiped using Blancco and the drive shredded into fragments and that a certificate of data destruction will be provided as an audit trail that this process has been completed.

The System Level Security Policy includes arrangements for data destruction through data shredding and physical destruction of disks. This is carried out by the IT Contractor.

Prior to the disposal, the server HDD are erased using PGPShred. The assets are then taken off site and physically destroyed by the IT Contractor. A video recording of the destruction is kept, as evidence that the asset has been destroyed. A list is maintained for assets that have destroyed including serial number for the HDD. The Audit Team noted that the University's contract with the IT Contractor did not cover the destruction of IT assets.

In the Audit Team's opinion the process documented in the System Level Security Policy on data destruction and hardware disposal is not consistent with the University of Nottingham requirement to use an approved waste disposal company that is WEEE compliant and provide destruction certificates for destroyed assets.

Conclusion: Hardware is not being disposed of in accordance with University policy, specifically the use of an approved waste disposal company.

2.5 Risk Assessment and Treatments

The University is committed to effective risk management of all its activities, at all its campuses. This commitment is demonstrated by embedding it in management processes, especially strategic planning, and through an integrated risk management framework involving risk identification, assessment, mitigation and assurance.

The Data Sharing Framework Contract and Data Sharing Agreement are with the University of Nottingham, and the University of Nottingham Council is ultimately responsible for risk management.

The Audit Team reviewed the risk assessment report for the project, which had been completed by an independent external consultant. The risk assessment was originally undertaken in March 2011 and updated on the 18th January 2016. The scope of the risk assessment covered the physical location of the systems (including the system for managing the salt), the research database system and server held files.

The University of Nottingham Risk Management policy states that

- units and projects that have local policies and risk register should ensure their local policy and practices align with the Risk Management policy;
- managers of major projects, and all other ventures which the University has a stake in, are obliged to identify, report, and manage risks that may have consequences for the University.

There was no documented evidence provided to support that:

- risk assessment methodology followed by the external consultant was aligned with the University of Nottingham policy;
- a local risk register existed;
- there was regular review of risks between April 2011 and December 2015.

Furthermore, the System Level Security Policy v1.0 originally submitted NIGB /Ethics and Confidentiality Committee/ DH security in 2011 stated that there would an annual risk assessment.

The University of Nottingham only requires escalation of risks to a school or university risk register where the department or project is unable to manage or accept the risk locally.

The Audit Team noted that an Information Asset Register is maintained by the Project Lead. The Asset Management Policy requires that information assets are classified based on the sensitive of the information they contain and detail on and risk assessments should be carried out on the assets. This had not been carried out on the HES information assets. Furthermore, there was no evidence to support that the Senior Information Risk Officer (SIRO) had been made aware of the HES information assets or details about the risk assessments. This is a requirement in the ICO Anonymisation: managing data protection risk - Code of Practice 2012.

Conclusions: Major weaknesses were identified in the execution of risk management on the project. Importantly, the sound governance controls defined by the University were not met.

3 Conclusions

Table 1 identifies the major nonconformities, minor nonconformities and observations raised as part of the audit.

Ref	Comments	Section in this Report	Designation
1.	The University of Nottingham used an IT Contractor as a data processor with full access to the system including all databases. There was no separation of duties for access to the HES data and the salt. Furthermore, whilst controls were in place, the Audit Team found that not all of the expected controls based on the ICO Anonymisation: managing data protection risk - Code of Practice 2012 were in place. The University of Nottingham and HSCIC have been reviewing and improving the controls in place over the lifetime of the data sharing arrangements. As an additional improvement, the University of Nottingham has transferred control of the salt to the data controllers. This means that the University of Nottingham no longer holds de-identified personal data.	2.1	Major
2.	No evidence was presented to show that the HES data are treated as de-identified personal data or had been assessed against the eight data protection principles. Furthermore the University's data protection registration entry did not include subjects of healthcare as a type of data subject. HES data that was not related to the population being studied was retained instead of being permanently deleted.	2.1	Major
3.	There was no documented evidence that a local risk register existed and there was no review of risks between April 2011 and December 2015.	2.5	Major
4.	There were differences in the System Level Security Policy and the Information Security Policy (and other University processes).This includes reporting of system breach to IT Services, using a WEEE approved contractor for IT asset disposal and ISO 27001 statement. The system is maintained by the IT Contractor and is not centrally controlled by IT Services, which is the basis of some of the controls in the Information Security Policy. The System Level Security Policy had not been reviewed and approved by University of Nottingham IT Services.	2.1	Minor
5.	A reference to the HSCIC guidance for reporting, managing and investigating information governance and cyber security serious incidents is added to the University guidance to ensure that appropriate reporting is initiated in the event of certain incidents occurring	2.1	Observation

Ref	Comments	Section in this Report	Designation
6.	There was no documented assessment confirming that non University laptops are used to carry out the processing of the data on the server had been assessed against the University of Nottingham's Desktop, Laptop and Mobile Security Policy to ensure they met configuration requirements. There was no reference in the Data Sharing Agreement or System Level Security Policy that laptops which were not University property would be used to access the HES data. Furthermore, the IT asset register does not include details of these laptops.	2.2	Minor
7.	The Audit Team found that there was no technical control enforcing minimum password length on two servers and the level of encryption one of the server holding the salt was 128bit, instead of 256 bit AES. The University's Encryption Policy recommends 256 bit AES encryption for long term security. The University of Nottingham Password Policy requires that the password is a minimum of seven characters and control mechanism enabled.	2.2	Minor
8.	A copy of the HES backup tape is taken off site and stored in a safe at a private, non-university location. Whilst this practice does not breaching the University of Nottingham's Backup Policy, there needs to be clear guidance on the offsite storage of backup tapes. This is also not fully explained in the System Level Security Policy.	2.2	Observation
9.	The secondary firewall between the University of Nottingham network and the servers where the HES data is stored was last patched in 2006, had reached end of life in December 2015 and is no longer supported (including security updates) by the manufacturer. In the absent of a network equipment patching policy, the Server Security policy requires that security patches must be installed on the system within seven days and the device should not be designated as 'end of life'. It should be noted that this is a secondary firewall behind the main University of Nottingham firewall and has been subjected to penetration testing.	2.3	Minor
10.	An external penetration test of the salt key server and the network for the servers holding HES data was commissioned and completed in January 2016. The independent report had been separated into two reports. The second part was made available to the Audit Team after the onsite visit and the University stated the first part of the report would only be made available after the recommendations had been implemented. The scale of these recommendations was not shared with the Audit Team. The Data Sharing Framework Contract clauses 7.3 and 7.4 require the data recipient provides information requested during an audit so that the HSCIC can verify compliance with the contract and agreement.	2.3	Minor
11.	The process documented in the System Level Security Policy on data destruction and hardware disposal is not consistent with the University of Nottingham agreement in that assets were not destroyed through a University of Nottingham approved WEEE contractor and suitable confirmation provided.	2.4	Minor

Ref	Comments	Section in this Report	Designation
12.	The University's Asset Management Policy requires that information assets are classified based on the sensitive of the information they contain and states risk assessments should be carried out on the assets. This classification and assessment had not been carried out on the HES information assets. Furthermore, there was no evidence to support that the Senior Information Risk Officer (SIRO) had been made aware of the HES information assets or details about the risk assessments.	2.5	Minor

Table 1: Nonconformities and Observations

3.1 Next Steps

University of Nottingham is required to review and respond to this report, providing corrective action plans and details of the parties responsible for each action and the timeline (based on priority and practicalities for incorporation into existing workload). As per agreement, review of the management response will be discussed by the Audit Team and validated at a follow-up meeting with the University of Nottingham. This follow-up will confirm whether the proposed actions will satisfactorily address the nonconformities and observations raised.

Following the onsite audit, a number of documents were updated or created by the University and forwarded to the Audit Team. These documents will be reviewed as part of the follow up process.