Guidance for Area Team Caldicott Guardians

Guidance for Area Teams Caldicott Guardians

National Health Applications and Infrastructure Services (NHAIS) – Process for the authorisation of Access Control Managers (ACMs)

Version number: 1.0

First published: August 2014

Prepared by: Wendy Harrison, NHAIS Information Project Lead

NHS England INFORMATION READER BOX		

Directorate		
Medical	Operations	**Patients and Information**
Nursing	Policy	Commissioning Development
Finance	Human Resources	

Publications Gateway Reference:	**02135**
Document Purpose	Guidance
Document Name	Guidance for Area Teams Caldicott Guardians
Author	W. Harrison
Publication Date	15 August 2014
Target Audience	All NHS England Employees
Additional Circulation List	
Description	This document is to inform Regional and Area Team Caldicott Guardians about the process which NHS England has implemented to facilitate the authorisation of Access Control Managers (ACMs) for the National Health Applications and Infrastructure Services (NHAIS) systems.
Cross Reference	None
Superseded Docs (if applicable)	None
Action Required	N/A
Timing / Deadlines (if applicable)	**Immediate**
Contact Details for further information	Stuart A Notholt Information Governance Communications Lead 07796994375

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet

Contents

1 Purpose

The purpose of this document is to inform Regional and Area Team Caldicott Guardians about the process which NHS England has implemented to facilitate the authorisation of **Access Control Managers (ACMs)** for the National Health Applications and Infrastructure Services (NHAIS) systems. In particular this process will ensure that appropriately authorised ACMs manage access requests to data within the NHAIS systems primarily via the Open Exeter portal of NHAIS but also including direct access and via the M-Connect and PCIS applications.

2 Scope

The document sets out the responsibilities delegated from the NHS England Caldicott Guardian, Sir Bruce Keogh, which enable NHS England to fulfil its obligations in terms of compliance with the law and statute. It also sets out the criteria for authorising Access Control Managers who will be responsible for managing access requests to data within NHAIS systems.

3 Audience

This guidance is aimed primarily at Area Team Caldicott Guardians and their nominated deputy. Regional Caldicott Guardians are included to ensure they are aware of the process and can support their Area Team Caldicott Guardians if required.

4 Compliance with legal and statutory functions

NHS England became the data controller for demographic primary care registration data and data controller in common with Public Health England in respect of Breast and Cervical Cancer Screening data from 1 April 2013[1].

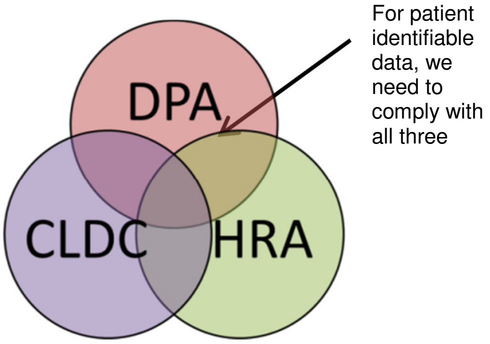
The Health and Social Care Information Centre (HSCIC) acts as data processor in the development and support of the NHAIS system and associated applications on behalf of NHS England, and Public Health England.

In the main, English NHAIS systems are managed by Primary Care Support Service (PCSS) teams within NHS England although in some areas this responsibility has been outsourced to third-party commercial organisations, for example NHS SBS and Serco who undertake this activity as part of a data processing contract on behalf of NHS England.

[1] Paragraph 14 of Schedule 6 of The National Health Service (General Medical Services Contracts) regulations 2004 [SI 2004/291] as amended by Regulation 27(8) The National Health Service (Primary Medical Services) (Miscellaneous Amendments and Transitional Provisions) Regulations 2013. http://www.legislation.gov.uk/uksi/2004/291/schedule/6/made and http://www.legislation.gov.uk/uksi/2013/363/regulation/27/made

In order that NHS England can enable appropriate access rights to English NHAIS data directly or via **Open Exeter, M-Connect or Organisation Links** an approval process is being implemented to ensure that NHS England takes full responsibility as the overall data controller for all data use requests. Each Area Team will be classed as an **Access Control Authority**, with Caldicott Guardians authorising new Access Control Managers for each of the NHAIS systems in their geographical area.

In order to process the personal data held within NHAIS, NHS England and Public Health England must meet the requirements of the Data Protection Act 1998 (DPA), the Access to Health Records Act 1990 (AtHR) for deceased records and the Human Rights Act 1998 (HRA). Additionally, if the data in question is confidential, then they must also satisfy the common law duty of confidence (CLDC). Where statute provides the legal basis for processing confidential patient information then this must either be stated explicitly or very clearly implied within the statutory provisions. Statute must be interpreted narrowly and minimising the interference with individuals' fundamental rights.


DPA
CLDC
HRA
For patient identifiable data, we need to comply with all three

Legal Framework

This effectively means that robust technical and organisational processes must be implemented to facilitate access to NHAIS data ensuring that only appropriate access is enabled and all access is provided in compliance with a sound legal basis.

5 NHAIS and associated (linked) systems

The NHAIS systems together form one of the largest databases in operation across the country. The Registration system manages in excess of 60 million records; it forms the core of an extensive primary care management base centred on a computerised index of NHS patients.

The Registration System contains the general identity details of patients registered with NHS GPs and is linked electronically with the Central Register held on the Central Health Record Inquiry System (CHRIS), managed by the National Back Office[2] (NBO) in Southport. NHAIS systems are also linked with and provide a direct feed to the Patient Demographic Service (PDS). Registration data provides the base used to calculate capitation payments to GPs, and is also used to identify patients for participation in screening programmes.

Given the wealth of information stored in the NHAIS systems there are many organisations that have historically relied on its data and will continue to require it in the new Health and Social Care landscape. Access has in the main been provided using the Open Exeter browser, from a data warehouse or local PMI created and maintained via Organisation Links or through the use of queries generated using M-Connect as a retrieval tool. Further information can be found via the following link: http://systems.hscic.gov.uk/ssd.

[2] Formerly known as the NHS Central Register (NHSCR).

6 Caldicott Guardian Responsibilities and summary role of ACMs

The delegated authority approved by the **NHS England Executive Management** (**EMT**) Team in May 2014[3] creates a responsibility for Area Team Caldicott Guardians to authorise Access Control Managers (ACMs) within their geographical area of responsibility. This will involve checking new ACM applications to ensure that the ACM role is appropriately assigned given that ACMs are in place to manage access requests to data within the systems primarily via the Open Exeter portal of NHAIS.

The ACMs will then use the Open Exeter Organisation Maintenance facility for adding new users or amending/deleting existing users in line with NHS England guidelines. The process will be supported by the HSCIC who will process the new Access Control Manager requests and set up appropriate permissions in accordance with the completed ACM application form as authorised by the Area Team Caldicott Guardians. Similarly, working with the Area Team Caldicott Guardian, the ACMs may be responsible for authorising at a local level[4]:

- new user accounts for operational purposes;
- new requests for M-Connect accounts;
- approval of ad-hoc or regular local data extracts;
- approval of access to Open Exeter for third-party providers (i.e. Non NHS care providers)[5]

Working with ACMs, the Area Team Caldicott Guardian may also be required to authorise local data extractions where it can be demonstrated that the request meets one of the criteria set out in the bullet points below or exceptionally, where there is no clear legal basis for providing NHAIS data and a decision on disclosure has to be made on the balance of public interests – that favouring disclosure against that of protecting public trust in the confidentiality of services. This requirement is in fact already part of the Caldicott Guardians functions as set out in the Caldicott Guardian Manual.[6]

For direct care, clearly identified data is needed for safe care. The legal basis for this is consent, which is implied as an integral part of the consent given for examination and treatment and the legal requirements to maintain health records[7].
For many other purposes it is feasible to use patient data in a form that does not enable individuals to be identified.

This requires investment in privacy enhancing methodologies[8] and technical solutions that utilise such methodologies that enable data to be linked and processed in de-identified form.

[3] ETM FABC - NHAIS ACM authorisation process approval request - Final v5 2014 05 20

[4] Local level refers to the NHAIS Cipher box(es) the ACM has access to

[5] Where the requestor is a 3rd party provider the NHS ATCG will be required to authorise the access request

[6] http://systems.hscic.gov.uk/infogov/links/2010cgmanual.pdf

[7] http://www.legislation.gov.uk/uksi/2004/291/schedule/6/made

In some instances it is not feasible to use anonymised[9] patient data for these other purposes. Where this is the case a legal basis for the use of identifiable patient data is needed. In these circumstances consideration must be given to whether:

H&SCA
2012
NHS Act
2006
Legal
framework

- there is a statutory basis that provides a secure legal basis to use identifiable patient data; or
- the Health and Social Care Information Centre (HSCIC) or Data Services for Commissioners Regional Office (DSCRO) could process the personal and confidential data to provide the data in an anonymised form; or
- it is feasible to obtain the consent of the individuals for the use of their personal confidential data; or
- the public interest justification for using identifiable patient data is sufficiently strong to warrant overriding the public interest of preserving public trust in the confidentiality of services and the personal interests of the individuals concerned[10].

In addition to ensuring there is a legal basis for processing, lawful processing also requires that the data are accurate and up to date and that only the minimum data necessary for the purpose are used. Additionally, appropriate organisational and technical measures to protect the data are needed. There are therefore a wide range of other information governance requirements that need to be met alongside ensuring there is a legal basis to process data. The **EMT** paper also sets out a requirement for an **Information Asset Owner** to be identified for each of the NHAIS boxes within the Area Team's geographical area.

The IAO responsibilities include ensuring compliance with technical security measures and associated audit requirements to support the Area Team's completion of their annual IG Toolkit assessment. Guidance which sets out the IAO role and responsibilities is available by clicking the following link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/255914/Guidance_on_the_IAO_Role.pdf however further guidance in relation to NHAIS systems will be provided to Information Asset Owners in due course.

[8] The methodologies are described in the Anonymisation for Publishing Health and Social Care Data standard and can be applied in other circumstances as well as publication, http://www.isb.nhs.uk/library/standard/128.

[9] Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place.
http://ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf

[10] This is called the public interest test. Routine data flows should not rely on public interest but need a secure basis in law.

7 Criteria for authorising Access Control Managers

Your responsibility as an Area Team Caldicott Guardian is to authorise **new** Access Control Managers working in organisations within your Area Team's geographical area which are either providing or supporting direct patient care. Access Control Managers in Primary Care Support Service (PCSS) teams are already in place and are responsible for setting up new users requiring access to NHAIS systems following strict authentication procedures set out by the HSCIC and NHS England. A list of currently identified Access Control Managers can be found below:

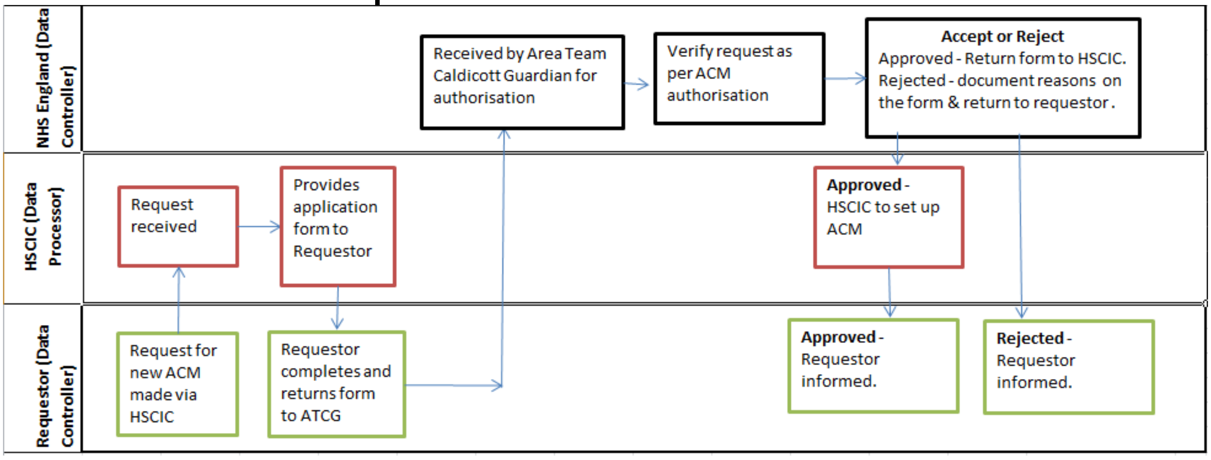
https://nww.openexeter.nhs.uk/nhsia/CipherQCodes/DataControllerList.jsp

8 Access Control Manager Verification process

Identify the following:

1. Check that the 0E60 form - **Request for NHAIS Access Control Manager (ACM) Rights** has been fully completed by the requestor? Is the requestor known to you? If not, check that your Area Team Primary Contact or Area Team Caldicott Guardian can verify the identity of the requestor.
2. Does the requestor have a role which is relevant to enabling access to NHAIS? Is the requestor of suitable seniority in the organisation? A relevant role is classified as one which carries a higher level of responsibility and understanding of the necessary access controls and assurance applicable to the use of Patient Confidential Data (PCD) within the organisation.
3. Verify that the requestor has provided a completion date confirming that their mandatory IG training is up-to-date. (All organisations working for or on behalf of the NHS must complete annual IG Training). This can be facilitated by using either the IG Training Tool or another training provider.
4. Once you have completed the checks above, and are happy to approve the application, sign the form, scan it and return via email to: exeter.helpdesk@hscic.gov.uk.
5. If you reject the ACM application, you should document your decision on the application form and return it to the requestor.

Outline of authorisation process:


NHS England (Data Controller)
HSCIC (Data Processor)
Requestor (Data Controller)
Request for new ACM made via HSCIC
Request received
Provides application form to Requestor
Requestor completes and returns form to ATCG
Received by Area Team Caldicott Guardian for authorisation
Verify request as per ACM authorisation
Accept or Reject
Approved - Return form to HSCIC.
Rejected - document reasons on the form & return to requestor.
Approved - HSCIC to set up ACM
Approved - Requestor informed.
Rejected - Requestor informed.

Completed forms should be emailed to: exeter.helpdesk@hscic.gov.uk

9 Glossary

Access Control Manager (ACM)	Previously known as ‘Operational Data Controllers’ within NHS organisations prior to enactment of the Health and Social Care Act 2012
Access Control Authority	Each Area Team will be classed as the Access Control Authority for their geographical area in respect of the NHAIS boxes within it.
Information Asset Owner (IAO)	Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process.
Cipher (NHAIS Boxes)	The encrypted hardware (server) which has a code to identify it is known as the Cipher.

10 Annexe A

See the embedded Excel Spreadsheet below for a list of all Cipher (Exeter Boxes) within Regional and Area Team Caldicott Guardian geographic area

NHAIS boxes by Regional & Area Teams 1

Microsoft Excel
97-2003 Worksheet