

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

Title	NOCA Information Governance Policy		
Document No.	POL 11		
Version No.	2		
Owner	Brid Moran, Information Manager, NOCA		
Authors	Cliona O'Donovan, Quality Assurance and Operations Manager, NOCA		
Reviewers	Fionnola Kelly, Head of Data Analytics and Research, NOCA Brid Moran, Information Manager, NOCA Aisling Connolly, Communications and Events Lead, NOCA Marina Cronin, Head of Quality and Development, NOCA		
Approved by	Ken Mealy on behalf of NOCA Governance Board		Level 1 Approval
Approved Date	08JUL22	Active Date	01AUG2022
Electronic Location	Q-Pulse		
Key Words	Information Governance, security, access, privacy, records management, data quality		
Change Log			
Version	List section numbers changed	Date	Author
	First version		
2	2.6.1.1 added	30MAY2022	C O'Donovan

This is a controlled document: While this document may be printed, the electronic version hosted in NOCA Q-Pulse is the controlled copy. A printed copy is only valid for 24 hours following download.

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

## TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>3</b>
1.1. Purpose.....	3
1.2. Scope .....	3
1.3. Objective .....	3
1.4. Outcome .....	4
1.5. Definitions.....	4
1.6. Roles and responsibilities .....	5
1.7. Supporting evidence .....	5
<b>2. APPROACH TO DEVELOPING NOCA INFORMATION GOVERNANCE POLICY .....</b>	<b>6</b>
2.1. Document statement .....	6
2.2. Procedural support .....	6
2.3. Approach to Information Governance (PRO 19) .....	6
2.4. Approach to Information Protection including security, privacy and confidentiality (PRO 20) .....	7
2.5. Approach to consent (PRO 21) .....	7
2.6. Approach to Access to data (PRO 22) .....	8
2.7. Approach to Records management and Retention (PRO 23) .....	9
2.8. Approach to Data Quality (PRO 24) .....	9
<b>3. MONITORING AND EVALUATION .....</b>	<b>9</b>
<b>4. REVISION /UPDATE .....</b>	<b>9</b>
<b>5. BIBLIOGRAPHY / REFERENCES .....</b>	<b>10</b>
<b>APPENDIX 1: DEVELOPMENT GROUP .....</b>	<b>13</b>
<b>APPENDIX 2: DISSEMINATION &amp; TRAINING PLAN .....</b>	<b>13</b>

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

## 1. INTRODUCTION

### 1.1. Purpose

This policy sets out an overarching framework for information governance in the National Office of Clinical Audit (NOCA), to ensure that information assets are managed effectively, in accordance with legislation and to a high standard. In addition, the policy makes staff aware of their responsibilities with regard to information governance, to create, develop and maintain a culture of information governance within the organisation and to outline the associated procedures that are available to assist them in achieving this objective.

### 1.2. Scope

1.2.1. This policy encompasses all information held by NOCA in order to carry out its business.

This includes but is not limited to:

- 1.2.1.1. Personal information i.e. relating to service users and employees
- 1.2.1.2. Corporate/Operational information e.g. contracts, service level agreements (SLA), financial information, human resources (HR) records, minutes of meetings, correspondence, emails etc.
- 1.2.1.3. Audit data e.g. minimum data sets, data dictionaries, raw data, aggregate data
- 1.2.1.4. Audit-associated data e.g. patient leaflets, consent forms, training manuals, training records
- 1.2.1.5. Supporting data e.g. continuing professional development (CPD) points, event feedback forms
- 1.2.1.6. Conflict of interest declarations of Board and committee members
- 1.2.1.7. The information held may be in different formats, both digital and hard copy. It includes information created in-house by staff and contractors and information received from third parties.

1.2.2. This policy applies to all staff employed by NOCA and any third parties carrying out work on NOCA's behalf.

### 1.3. Objective

The objective of this policy is to ensure that all data and information processed by NOCA are

- 1.3.1. Processed lawfully, fairly and transparently
- 1.3.2. Collected for specific purpose and not further processed in a manner that is incompatible with the original purpose
- 1.3.3. The minimum that are required and that no unnecessary information are collected
- 1.3.4. Accurate, high quality and up to date
- 1.3.5. Stored securely and confidentially
- 1.3.6. Not stored for any longer than necessary
- 1.3.7. Subject to access controls where access is provided to authorised users only
- 1.3.8. Protected, data protection is considered by default for all data collections

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

## 1.4. Outcome

The outcomes of implementation of this policy are:

- 1.4.1. That there are robust structures in place to monitor and evaluate the effectiveness of NOCA's information governance processes.
- 1.4.2. That there is evidence of NOCA's compliance with all relevant legislation and best practice standards.
- 1.4.3. That audit data governed by NOCA are fit for purpose and can be reliably used in the improvement of health services to patients.
- 1.4.4. To provide public assurance that data governed by NOCA are accurate and managed ethically.

## 1.5. Definitions

**Table 1.1: Definitions used in this document**

Term	Meaning
Aggregate data	Data that are derived from aggregating record-level data, for example average length of stay per hospital is derived by calculating the average from individual cases' length of stay. This type of information will not routinely allow direct identification of individuals or entities
Anonymous data	Data collected without identifiers such as name, address, or date of birth that can never be linked to an individual (HSE, 2013)
Audit processor	Organisation to whom audit data is submitted and who analyses the audit data for national clinical audit.
Conflict of Interest	set of circumstance that creates a risk that professional judgement or actions regarding a primary interest will be unduly influenced by a secondary interest (Institute of Medicine, 2009, P. 46)
Data Quality	Evidence illustrating that data is fit for purpose. The quality of data can be determined through assessment against internationally accepted dimensions (Health Information and Quality Authority, 2018).
De-identified data	Data are separated from personal identifiers, for example, through the use of a link, e.g. a code. Access to the link is strictly controlled. As long as a link exists, data are considered indirectly identifiable as opposed to being anonymous (HSE, 2013)
Derived data	Data are that are derived from other pieces of data, for example length of stay may be derived from date of admission and date of discharge
Information Asset	A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles (The National Archives, 2017).
Information Governance	Arrangements that service providers have in place to manage information to support their immediate and future regulatory, legal, risk, environmental and operational requirements (Health Information and Quality Authority, 2012).
National Clinical Audit	National clinical audit is a cyclical process that aims to improve patient care and outcomes by systematic, structured review and evaluation of clinical care against explicit clinical standards on a national basis. (National Clinical Effectiveness Committee, 2015)
Personal Data	Information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological,

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

Term	Meaning
	genetic, mental, economic, cultural or social identity of that natural person (GDPR, Article 9, 1).
Privacy by default	ensures that for any activity, process or product that involves data processing, the default settings are always the most privacy-friendly ones. (Health Research Board, 2019).
Privacy by Design	where privacy is considered from the initial concept and design of any activity, process or product that involves data processing (e.g. a research project) right throughout its lifecycle through to its conclusion (including considerations of data erasure and/or archiving) (Health Research Board, 2019).
Record level data	Record level data contain information about a unit of observation (HPO, 2015) . Where these data refer to an individual, these data are deemed sensitive and will be anonymised prior to release for specialist users only (e.g. researchers)
Research	Systematic inquiry that uses disciplined methods to answer questions or solve problems. The purpose of clinical research is to develop, refine and expand the base of knowledge (Polit & Beck, 2006).
Secondary Use of Information	relates to information collected in the course of providing care being used for purposes other than direct service user care such as audit, performance report, service planning, and research”( Health Information and Quality Authority, 2012b).
Special Categories of Personal Data	personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (GDPR, Article 9, 1).

## 1.6. Roles and responsibilities

**Table 1.2: Roles and responsibilities**

Role	Responsibility
<i>NOCA Governance Board</i>	The NOCA Governance Board is responsible for reviewing and approving this policy
<i>NOCA Executive Director</i>	The NOCA Executive Director is responsible for reporting to the Governance Board on issues relating to information governance
<i>NOCA Information Manager</i>	The NOCA Information manager has overall responsibility for the NOCA approach to information governance, for ensuring this policy complies with regulatory obligations and for the implementation of this policy.
<i>Department Heads/Audit Managers</i>	Department Heads/Audit managers are responsible for ensuring that information assets under their control are managed in compliance with this policy and related procedures
<i>NOCA staff</i>	All NOCA staff have responsibility to ensure that they always comply with this policy and related procedures

## 1.7. Supporting evidence

Legislation, standards and guidelines that support this policy include, but are not limited to:

- [Data Protection Act 2018](#)
- [Data Protection Acts 1988 and 2003](#)
- [the 2011 “ePrivacy Regulations” \(S.I. No. 336 of 2011 – the European Communities \(Electronic Communications Networks and Services\) \(Privacy And Electronic Communications\) Regulations 2011\)](#)
- [Freedom of Information Act 2014](#)

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

- [General Data Protection Regulation \(EU\) 2016/679 \(GDPR\)](#)
- [Health Information and Quality Authority \(HIQA\), \(2012\) National Standards for Safer Better Healthcare.](#)
- [Health Information and Quality Authority. \(2017\). Information management standards for national health and social care data collections](#)
- [Health Information and Quality Authority. \(2018\). Guidance on a data quality framework for health and social care](#)

## 2. Approach to developing NOCA Information Governance Policy

### 2.1. Document statement

The NOCA Information Governance policy is applicable to all NOCA staff and to all information assets managed by NOCA. Compliance with this policy is mandatory.

### 2.2. Procedural support

This policy document is supported by:

- 2.2.1.PRO19 NOCA procedure on good governance of Information including Privacy Impact assessment
- 2.2.2.PRO20 NOCA procedure on Information Protection including Security, Privacy and Confidentiality
- 2.2.3.PRO21 NOCA Procedure on Consent
- 2.2.4.PRO22 NOCA procedure on Access to Data managed by NOCA
- 2.2.5.PRO23 NOCA Procedure on Records Management and Retention
- 2.2.6.PRO24 NOCA Procedure on Data Quality

### 2.3. Approach to Information Governance (PRO 19)

- 2.3.1.NOCA procedure good governance of Information describes procedural steps so that staff at all levels of the organisation are aware of their responsibilities and accountability for information governance. Details of the levels of responsibility and accountability between roles are clearly delineated.
- 2.3.2.NOCA ensures that any data collected are collected for a specific, valid reason
- 2.3.3.Key performance indicators (KPI) against which the quality of its information governance processes are measured are described. Audits of compliance of NOCA's information governance approach are carried out on a regular basis.
- 2.3.4.Reports on information governance issues are on the agenda of the NOCA Governance Board and NOCA Executive Team meetings.
- 2.3.5.Information Governance training is provided for all staff as a mandatory part of staff induction programmes. In addition, regular refresher training on all aspects of information governance are provided and managed through NOCA's quality

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

management system, Q-Pulse. Training may be role specific. Records of training attendance and competency assessment are maintained in Q-Pulse.

- 2.3.6. NOCA maintains an information asset register. This is reviewed and updated annually and inform records management and data retention policies.
- 2.3.7. NOCA publishes a statement of information practices for each audit so that service users are aware of their rights with regard to how information held about them is collected, used and protected.
- 2.3.8. NOCA conducts and documents Privacy Impact Assessments
- 2.3.9. NOCA ensures that procedures and processes are in place to implement the procedure, including processes to manage breaches.
- 2.3.10. NOCA publishes the NOCA approach to Information Governance (this document) via the NOCA website.

## 2.4. Approach to Information Protection including security, privacy and confidentiality (PRO 20)

- 2.4.1. NOCA maintains procedures in order to ensure that the organisation is compliant with relevant legislation and best practice standards with regard to data protection.
- 2.4.2. A Data Protection Impact Threshold Assessment is carried out for all projects.
- 2.4.3. NOCA undertakes a full Data Protection Impact Assessment (DPIA) when required, particularly when a new IT system or new use of data resulting in high-risk processing, any major change to an existing IT system or use of data, and when commencing a new data collection
- 2.4.4. NOCA maintains a device asset register. This is reviewed and updated as new devices are purchased or existing devices re-allocated in line with staff starters and leavers
- 2.4.5. NOCA maintains privacy and confidentiality procedures that are compliant with relevant legislation and best practice standards.
- 2.4.6. Privacy by design and by default will be incorporated into all future specifications for projects, applications and systems.
- 2.4.7. NOCA maintains procedures in order to ensure that the organisation meets the three objectives of information security:
  - 2.4.7.1. Confidentiality – access to information assets and data are restricted to authorised users only
  - 2.4.7.2. Integrity – all information is complete and accurate and information systems operate in accordance with their specification.
  - 2.4.7.3. Availability – information and information systems are available to authorised users when they are needed.

## 2.5. Approach to consent (PRO 21)

- 2.5.1. If the legal basis for the collection of data requires consent, then NOCA will obtain the data subject's full informed consent in advance.
- 2.5.2. Examples where consent is required include
  - 2.5.2.1. Patient registers e.g. INOR
  - 2.5.2.2. collection of personal information through the website

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

- 2.5.2.3. collection of person's image
- 2.5.3. implied consent is considered at NOCA events such as conferences by providing information in advance that photography will be used
- 2.5.4. consent for use of identified photographs in NOCA publications will be sought in advance of any use
- 2.5.5. children's photographs will not be used without permission of the child's guardian
- 2.5.6. patient stories, in writing and in video format
- 2.5.7. consent for use of subject identifiable data in research

## 2.6. Approach to Access to data (PRO 22)

- 2.6.1. NOCA abides by the principle of sharing data appropriately. In addition to disseminating insights from the data under NOCA governance, NOCA endeavours to provide access to non-personal high value datasets through Ireland's Open Data portal at data.gov.ie and NOCA responds to Data Access Requests.
  - 2.6.1.1. When responding to data requests, the starting point is to release data unless there is a valid reason not to. Valid reasons for non-release include but are not limited to data are not held by NOCA, NOCA do not have the right to share the requested data, requested data cannot answer the question the requestor is asking, data are insufficient quality for the intended use, data will be published imminently by NOCA, release of the data would identify an individual.
- 2.6.2. Data Access requests may come to NOCA for various purposes including but not limited to the categories listed below:
  - 2.6.2.1. Subject Access request under GDPR where a person may request to know what data NOCA holds about that person
  - 2.6.2.2. Freedom of Information Requests
  - 2.6.2.3. Data Access Request for service evaluation and quality initiatives
  - 2.6.2.4. Data Access request for research
  - 2.6.2.5. Media queries
  - 2.6.2.6. Parliamentary questions
- 2.6.3. NOCA will not disclose patient identifying information except in relation to INOR; then only to support an implant recall or directly to a patient if a data subject access request is received.
- 2.6.4. All data access requests are logged and requestor details are stored
- 2.6.5. All data access requests are examined and categorised as above
- 2.6.6. All data access requests are considered under the legal basis for the collection of that data
- 2.6.7. Depending on the type of data requested, before providing data NOCA may require the requestor to demonstrate that they have appropriate governance in place to manage that data.

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

## 2.7. Approach to Records management and Retention (PRO 23)

- 2.7.1. Applicable to all data generated by, stored, collected and processed by NOCA, in any format
- 2.7.2. Data are not stored for longer than is necessary
- 2.7.3. Retention periods are grouped by type of record held
- 2.7.4. NOCA will conduct an annual review of the retention of records

## 2.8. Approach to Data Quality (PRO 24)

- 2.8.1. High quality data indicates data that are fit for purpose (HIQA, 2018). This procedure describes NOCA processes to provide assurance on data quality
- 2.8.2. NOCA works with data providers to assess and improve the quality of data provided
- 2.8.3. All data handling is performed in ways that ensure data are not corrupted by data access, transformation, analysis, presentation

## 3. Monitoring and Evaluation

- 3.1. Compliance with this policy is monitored on an ongoing basis as part of NOCA quality assurance of audit report development and annually as part of NOCA's annual audit of GDPR compliance
- 3.2. This policy will be evaluated by examining the number of planned and unplanned deviations, change requests raised on this policy and the associated procedures.

## 4. Revision /Update

This policy will be reviewed within two years of its active date in accordance with PRO 2 *Procedure for document management in NOCA*

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

## 5. Bibliography / References

Data Protection Commission (2019a). *Guidance for Controllers on Data Security* [Online]. Dublin: DPC. Available: <https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190625%20Data%20Security%20Guidance.pdf> [Accessed 1 December 2019].

Data Protection Commission (2019b). *Quick guide to the principles of data protection* [Online]. Dublin:DPC. Available: [https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection\\_Oct19.pdf](https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf). [Accessed 1 December 2019].

Health Information and Quality Authority. (2017a). *Guidance on Privacy Impact Assessment in health and social care. Version 2.0* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf> [Accessed 1 December 2019].

Health Information and Quality Authority. (2017b). *Information Governance Self-Assessment Tool* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/sites/default/files/2017-01/IG-Self-Assessment-Form.pdf> [Accessed 1 December 2019].

Health Information and Quality Authority. (2017c). *Information management standards for national health and social care data collections* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/sites/default/files/2017-02/Information-management-standards-for-national-health-and-social-care-data-collections.pdf> [Accessed 1 December 2019].

Health Information and Quality Authority. (2017d). *Self-assessment tool for national health and social care data collections* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/sites/default/files/2017-05/Self-Assessment-Tool-for-national-health-and-social-care-data-collections-May2017.pdf> [Accessed 1 December 2019].

Health Information and Quality Authority. (2010). *Guidance on Privacy Impact Assessment in Health and Social Care* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf> [Accessed 1 December 2019].

Health Information and Quality Authority. (2011). *What you should know about information governance: a guide for health and social care staff* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/sites/default/files/2017-01/Information-Governance-Guide.pdf> [Accessed 1 December 2019].

Health Information and Quality Authority. (2012a). *Guidance on information governance for health and social care services in Ireland* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/sites/default/files/2017-01/Guidance-on-information-governance.pdf> [Accessed 24 November 2019].

Health Information and Quality Authority. (2012b). *National Standards for Safer Better Healthcare* [Online]. Dublin: HIQA. Available: <https://www.higa.ie/reports-and-publications/standard/national-standards-safer-better-healthcare> [Accessed 1 December 2019].

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

Health Information and Quality Authority. (2017). *Information management standards for national health and social care data collections* [Online]. Dublin: HIQA. Available: <https://www.hiqa.ie/sites/default/files/2017-02/Information-management-standards-for-national-health-and-social-care-data-collections.pdf> [Accessed 1 December 2019].

Health Information and Quality Authority. (2018). *Guidance on a data quality framework for health and social care* [Online]. Dublin: HIQA. Available: <https://www.hiqa.ie/sites/default/files/2018-10/Guidance-for-a-data-quality-framework.pdf> [Accessed 1 December 2019].

Health Research Board. ([2019]). *Privacy by design and default* [Online]. Dublin: HRB. Available: <https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-overview/gdpr-principles/privacy-by-design-and-default/> [Accessed 1 December 2019].

Health Service Executive. (2011). *Standards and Recommended Practices for Healthcare Records Management V3.0 (QPSD-D-006-3)* [Online]. Dublin: Health Service Executive. Available: <https://www.hse.ie/eng/about/who/qid/quality-and-patient-safety-documents/v3.pdf> [Accessed 1 December 2019].

Health Service Executive. (2013a). *Information Classification & Handling Policy* [Online]. Dublin: HSE. Available: <https://www.hse.ie/eng/services/publications/pp/ict/information-classification-handling-policy.pdf> [Accessed 11 December 2019].

Health Service Executive. (2013b). *Information Technology (I.T.) Security Policy* [Online]. Dublin: Health Service Executive. Available: <https://www.hse.ie/eng/services/publications/pp/ict/information-security-policy.pdf> [Accessed 28 November 2019].

Health Service Executive. (2019a). *National Consent Policy V. 1.3* [Online]. Dublin: HSE. Available: <https://www.hse.ie/eng/about/who/qid/other-quality-improvement-programmes/consent/national-consent-policy-hse-v1-3-june-2019.pdf> [Accessed 1 December 2019].

Healthcare Quality Improvement Partnership. (2017). *Information governance in local quality improvement* [Online]. London: HQIP. Available: <https://www.hqip.org.uk/wp-content/uploads/2018/02/information-governance-in-local-quality-improvement.pdf> [Accessed 30 November 2019].

Information Governance Alliance. (2016). *Records Management Code of Practice for Health and Social Care* [Online]. IGA. Available: <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016> [Accessed 1 December 2019].

International Organization for Standardization. (2016). *ISO 15489-1:2016. Information and documentation — Records management — Part 1: Concepts and principles* [Online]. Geneva: ISO. Available: <https://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-2:v1:en> [Accessed 1 December 2019].

International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements* [Online]. Geneva: ISO. Available: <https://www.iso.org/standard/75106.html> [Accessed 1 December 2019].

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

Kelleher, D. & Murray, K. (2018). *EU Data Protection Law*, Dublin, Bloomsbury.

NHS. (2019). *Information Governance Policy. V 5.1* [Online]. Available:  
<https://www.england.nhs.uk/wp-content/uploads/2019/10/information-governance-policy-v5.1.pdf>  
[Accessed 1 December 2019].

The National Archives. (2017). *Information asset factsheet* [Online]. London: TNA. Available:  
<https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf> [Accessed 1 December 2019].

Document Name	Information Governance Policy
Document No	POL 11
Version No	2
Active Date	01AUG2022

## APPENDIX 1: DEVELOPMENT GROUP

Name	Title	Role
Brid Moran	Information Manager	Owner
Cliona O'Donovan	QA and Ops Manager	Author
Fionnola Kelly	Head of Data Analytics and Research	Reviewer
Marina Cronin	Head of Quality and Development	Reviewer
Aisling Connolly	Communication and Events Lead	Reviewer

## APPENDIX 2: DISSEMINATION & TRAINING PLAN

This controlled document is disseminated to NOCA staff through Q-Pulse

The following table sets out the dissemination and training provisions associated with this template.

### A2.1 Plan

Plan Elements	Plan Details	
The Dissemination Lead is	Quality and Operations Manager	
This document replaces existing documentation	Yes	
This document is to be disseminated to	All NOCA Staff	
Training requirement	ALL NOCA staff	Level 1
The Training Lead	Information Manager	
Additional Information	Controlled document retained on Q Pulse	

### A2.2: Training assessment

Who?	All identified with level 1 training requirement complete this training assessment
Compliance against?	POL 11 Information Governance Policy
Outcome?	Competence requires $\geq 80\%$ on the training assessment
<b>Questions</b>	
1. Does the scope of this policy include non-audit related data that is held by NOCA?	
2. Identify 3 objectives of this policy	
3. Define the term Anonymous data	
4. Define the term Personal data	
5. Define the term Aggregate data	
6. What are the differences between clinical audit and research?	
7. Who is responsible for compliance with this policy?	
8. Name the 6 procedures that must be complied with in order to comply with this policy	

### A2.3: Training Log

Training in this controlled document is documented within Q-Pulse