Information Governance Management Framework

<table>
<thead>
<tr>
<th>Responsible Officer</th>
<th>Business Planning &amp; Resources Director</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>Governance Manager</td>
</tr>
<tr>
<td>Date effective from</td>
<td>October 2015</td>
</tr>
<tr>
<td>Date last amended</td>
<td>October 2015</td>
</tr>
<tr>
<td>Review date</td>
<td>October 2018</td>
</tr>
<tr>
<td>Audience</td>
<td>NICE Board and staff (including contractual staff)</td>
</tr>
</tbody>
</table>
Introduction

1. The Information Governance Management Framework sets out the standards to be applied for managing information governance including the organisational arrangements, roles, responsibilities and policies.

2. Information governance covers the framework of law and best practice within which information is managed in a confidential, consistent and secure manner. Particular focus is placed on the management of personal data and other confidential information including commercially sensitive submissions from industry to ensure it is handled legally, securely and efficiently in accordance with business needs.

3. NICE uses the Security Policy Framework (SPF) to benchmark its standards for information governance and its performance is reported to the Department of Health.

Scope

4. This framework applies to all NICE staff and the following groups of people who work for or on behalf of NICE. This document describes these (non-staff) groups collectively as ‘affiliates’:
   - committee chairs and members, and remunerated expert advisers
   - non-executive directors
   - agency workers and contractors on temporary contract or employed through an agency to work for NICE
   - secondees (those who are seconded to NICE from other organisations)
   - unpaid student, volunteers or placement staff

Principles

5. The standards for information governance encompass openness, legal compliance and information security with a particular focus on the management of personal data.

6. Openness and transparency will be promoted via the website and through the Publication Scheme and will apply an appropriate balance between openness and confidentiality in the management and use of information.

7. Effective standards of confidentiality and data protection are applied to staff and affiliates through policies, procedures and training and in accordance with legislative requirements.

8. Strong information security arrangements are applied to safeguard personal information about staff and affiliates, those we do business with, and to commercially sensitive and other confidential information.
Reporting standards

9. The Department of Health requires assurance from NICE that its standards are adequate and proportionate to its information risks. This information is captured in an annual information governance report to the Senior Management Team and Audit and Risk Committee which is benchmarked against the standards set out in the Security Policy Framework (SPF).

10. The SPF is a high level approach to information governance that is used across government and which identifies the key standards to be met to ensure effective information security.

11. Where appropriate enhanced levels of information controls are applied to sensitive information supplied by partners and stakeholders.

Information risk

12. Arrangements for managing information risk are incorporated into the NICE Risk Management Policy which incorporates risk identification, assessment, escalation, and mitigation. Information risk management is informed by NICE’s risk appetite and all mitigating actions and controls are designed to be proportionate to the risks faced by NICE.

13. The Senior Management Team identify and collectively manage risks on behalf of the Board. Directors manage information risks within their centre/directorate, supported by the designated information asset owners (IAOs)\(^1\).

14. The Senior Management Team and Audit and Risk Committee receive an annual report on information governance each October which includes an assessment of compliance against the SPF.

Health and Social Care Information Centre data

15. Specific contractual arrangements are in place for information received from the Health and Social Care Information Centre (HSCIC) including Hospital Episode Statistics (HES) data, and this is managed within the Health and Social Care Directorate. A dedicated process manual sets out standards to manage access to HSCIC data on a ‘need-to-know’ basis and to ensure it is managed with enhanced controls. This is subject to periodic spot checks and monitoring.

16. NICE uses a variety of data sources during the development of its guidance and the HSCIC provide access to bespoke data extracts and full access to the HES data warehouse. The data NICE receives is either anonymised or pseudo-anonymised and there is little risk of an individual being re-identified.

\(^1\) Further information on roles and responsibilities is set out in paragraphs 21 to 29
Information assets

17. An information asset is a body of information managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

18. Taking care of information assets supports information governance and enables NICE to ensure that sensitive personal data and confidential information is handled legally, securely and efficiently in accordance with business needs. It ensures the management of information supports the efficient location and retrieval of corporate records where and when needed.

19. The HES database, Board papers, guidance development records, and appeal papers are all examples of information assets. A register of information assets is maintained by the Governance Manager with support from IAOs.

20. It will be the responsibility of each IAO to identify what information assets are held within their area of responsibility, and to ensure this is documented in their Directorate’s Information Asset Register which will form part of the NICE register.

Roles and responsibilities

21. The NICE Board retains overall responsibility for risk management. The Audit and Risk Committee reviews incident reports, receives an annual report on information governance and considers reports from internal audit on the assurances relied upon to manage information risk.

22. The Chief Executive, as Accounting Officer, has overall responsibility for information governance and provides appropriate assurance through the governance statement in the annual report that information risks are effectively managed and mitigated to an acceptable level. The main responsibilities in relation to information governance are set out in appendices 1-5.

23. The Business Planning and Resources Director is the Senior Information Risk Owner (SIRO) and advises the Accounting Officer on information risk. The SIRO is responsible for the management of information risk at Board level and the specific duties are set out in appendix 2.

24. The Deputy Chief Executive is the Caldicott Guardian and has a particular focus on managing the confidentiality, security and sharing of patient information and the responsibilities are set out in appendix 3.

---

2 National Archives
3 Cabinet Office guidance on mandatory roles
25. The Governance Manager is responsible for the day to day management of information governance and coordinates NICE’s overall information risk approach. The role provides professional advice on the application of information access legislation including the Freedom of Information Act 2000 and Data Protection Act 1998 and produces an annual information risk report. The Governance Manager also coordinates the work of the Information Asset Owners (IAO) to ensure information assets are effectively managed. The specific responsibilities are set out in appendix 4. The Governance Manager reports to the Associate Director, Corporate Office whose responsibility for delivering an efficient corporate governance function includes information governance and risk assurance.

26. Information Asset Owners (IAO) are responsible for the management of information held in their team including who has access to sensitive information. They understand and address risks to the information in their teams, and escalate issues as required to the Governance Manager. Their responsibilities are set out in appendix 5.

27. The Records and Information Manager is responsible for ensuring a planned approach to records management across NICE to support information governance and coordinates the work of the records leads in each team.

28. SMT have approved an Information Governance Steering Group to coordinate information governance compliance across NICE, with responsibility for leading the implementation and monitoring of the SPF. The group is chaired by the Governance Manager. Its terms of reference are set out in appendix 6.

29. All staff and affiliates have a responsibility to comply with NICE policies, protect the security of confidential information, and undertake training as required. If necessary advice should be obtained from their line manager, IAO or the Governance Manager.

30. The structure for information management at NICE agreed by SMT is set out below:
Incident management

31. Information incidents are reported in accordance with the Incident Reporting Policy and escalated as necessary to the Senior Management Team, Audit and Risk Committee or Department of Health depending on their severity. Reports to the Audit and Risk Committee include a synopsis of the nature of the incident, why it occurred together with ‘lessons learnt’ and associated actions needed to minimise the risk of recurrence.

32. Incidents are monitored to identify any systemic risks and to ensure appropriate remedial action and is taken and effective controls put in place.

Information assurance

33. Internal audit periodically review key aspects of information governance at NICE and report to the Audit and Risk Committee on the suitability of controls to manage risks and make recommendations for additional actions where needed.

Contracts

34. All contracts with third parties managing personal data or confidential information on behalf of NICE include standard information security clauses relating to the safe handling of that data.
Cyber security and business continuity

35. NICE IT apply a comprehensive set of controls to the internal NICE IT network to ensure resilience and disaster recovery in the event of temporary or partial outages of IT systems and these are replicated across both sites. The full set of controls and disaster scenarios has been reported to the Audit and Risk Committee.

36. NICE complies with the '10 steps to cyber security' recommended by the Cabinet Office to baseline cyber security standards at NICE.

37. Portable media are encrypted where appropriate. Details are set out in the Information Technology Policy.

38. Penetration testing is conducted periodically to test the resilience of IT systems and external consultancy support engaged where necessary.

Training

39. Information governance training must be completed by all staff using the Civil Service Training module or equivalent and new staff are advised of this requirement at induction. Information Asset Owners complete the module for IAOs and the Senior Information Risk Owner and Governance Manager have undertaken additional external training.

40. Training only needs to be completed once and additional refresher training is conducted as necessary where there is an identified need.

41. Staff handling data from the Health and Social Care Information Centre undertake specific training provided by the HSCIC.

42. Training is supplemented by good practice guides on information governance and central support and advice from the Governance Manager.

Confidentiality

43. Information received by NICE may be confidential even if it not marked as such. Staff are obliged to keep all sensitive personal data and confidential material secure and a breach of this obligation may constitute a disciplinary offence in accordance with NICE policies.

Sharing personal data

44. Data sharing is managed in accordance with NICE data sharing protocols to protect the privacy and confidentiality of personal data held by NICE taking account of relevant legislation and guidance from the Information Commissioner’s Office.

45. In all cases personal data will be shared securely and strictly on a need to know basis and the information restricted to the minimum required for the task.
Records management

46. NICE ensures a systematic and planned approach to records management from creation to ultimate disposal to support information governance and ensures adequate records are maintained, managed and controlled commensurate with legal, operational and information needs.

47. Dedicated systems will be developed to manage guidance development information with associated industry standard records and information protocols.

Communication

48. Information is communicated to staff via the Information Governance Steering Group, which includes all Information Asset Owners, and cascaded to individual teams for action.

49. The intranet is utilised to provide a centralised resource and point of reference for staff for information governance and records management including policies, good practice guides and key contacts.

Related policies
- Data Protection Policy
- Information Technology Policy
- Risk Management Policy
- Incident Reporting Policy (under review)
- Freedom of Information Policy and Complaints Procedure
- Records Management Policy
- Email & Internet Policy
- Information Charter
- Data Sharing Protocols
Appendix 1

**Accounting Officer**

1. The Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks.

<table>
<thead>
<tr>
<th>Aspect of role</th>
<th>Supporting actions</th>
</tr>
</thead>
</table>
| Lead and foster a culture that values, protects and uses information for the public good | • have a SIRO who is skilled, focused on the issues, and supported  
• review and encourage organisational plan to achieve and monitor the right culture  
• take visible steps to support and participate in that plan (including completing own training) |
| Discuss information risk in the delivery chain where necessary with the Board | • Audit and Risk Committee discusses the quarterly risk assessments and annual forward look  
• The Audit and Risk Committee discusses breaches and “near misses”, to learn lessons and share them with others |
| Cover information risk explicitly in the governance statement                 | • receive an annual assessment of information risk performance from the Governance Manager, that draws on material from information asset owners and specialists  
• publish summary material in the annual governance statement                   |

---

4 Accounting Officer, SIRO, IAO, Head of Knowledge/Information Management Cabinet Office template
**Appendix 2**

**Senior Information Risk Owner**

2. The SIRO is an executive familiar with information risks and leads the organisation’s response. The SIRO is the focus for the management of information risk at Board level.

<table>
<thead>
<tr>
<th>Aspect of role</th>
<th>Supporting actions</th>
</tr>
</thead>
</table>
| Lead and foster a culture that values, protects and uses information for the public good | • ensures the organisation has measures that are proportionate to the risks faced by the organisation  
• takes visible steps to support and participate in that plan (including completing own training) |
| Own the overall information risk policy and risk assessment process, test its outcome, and ensure it is used | • ensures that risk policy is complete – covering how the organisation implements proportionate measures in its own activity and that of delivery partners  
• ensures that risk assessment is completed at least quarterly, based on the risk assessment understands what information risks there are to the organisation through its delivery chain, and ensures that they are addressed  
• ensures that risk assessment and actions taken benefit from an adequate level of independent scrutiny |
| Advise the accounting officer on the information risk aspects of his governance statement | • receives annual assessment of performance, covering proportionate measures as well as actions planned for the organisation’s own circumstances  
• provide advice to Accounting Officer on the information risk parts of their governance statement |
Appendix 3

Caldicott Guardian

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of a patient and service-user information and enabling appropriate information-sharing.

All organisations that have access to patient records must have a Caldicott Guardian.

The Guardian plays a key role in ensuring that organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation in relation to information governance, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

\[^{5}\text{HSCIC}\ http://systems.hscic.gov.uk/data/ods/searchtools/caldicott/index.html\]
### Governance Manager

3. The Governance Manager is responsible for co-ordinating the organisation’s overall information risk approach, ensuring that professional support and advice is offered to the business, including Information Asset owners, and ensuring that information is managed as an asset. The role will include:

<table>
<thead>
<tr>
<th>Aspect of Role</th>
<th>For example shown by</th>
</tr>
</thead>
</table>
| Leads and fosters a culture that values, protects and uses information for the public good. | • Provides professional expertise in relevant legislation (FOI, Public Records Act, Data Protection, re-use, etc) ensuring that everyone understands their legal obligations and realises potential opportunities.  
• Prepares the annual information governance report for the Senior Management Team and Audit & Risk Committee and ensures work is coordinated and implemented. (e.g. manages the training, ongoing induction, etc).  
• Ensures the organisation has IAOs who are skilled, focussed on the issues, and supported, plus the specialists that it needs  
• Stays well networked in the wider community to ensure that the organisation always learns from good practice elsewhere. |
| Prepares and develops the overall Information Risk Policy and assessment process and keeps it current and relevant. | • Prepares the assessment of risk, working alongside business users and using best practice.  
• Advises the SIRO on major risks and their potential impact and mitigation.  
• Ensures that new risks are understood and managed.  
• Owns the day-to-day management of the framework and process. |
| Ensures that information assets are fully used for the public good, including responding to requests for access from others. | • Maps key assets held by organisation overall.  
• Coordinates the work of Information Asset owners (IAO) to ensure that IAOs understand their legal and regulatory framework, share common approaches and learn from each other.  
• Assesses opportunities and risks based on request logs and other analysis, taking overview across the organisation.  
• Reports recommendations to SIRO and SMT to ensure Board visibility of opportunities and costs.  
• Manages the Records and Information Manager to ensure records are managed to acceptable standards to support information governance |
Appendix 5

Information Asset Owner

4. Information asset owners are senior individuals from across the Institute. 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.

<table>
<thead>
<tr>
<th>Aspect of role</th>
<th>Supporting actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead and foster a culture that values, protects and uses information for the</td>
<td>• understands the organisation’s plans to achieve and monitor the right culture,</td>
</tr>
<tr>
<td>public good</td>
<td>across the organisation and its partners</td>
</tr>
<tr>
<td></td>
<td>• takes visible steps to support and participate in that plan (including completing</td>
</tr>
<tr>
<td></td>
<td>own training)</td>
</tr>
<tr>
<td>Knows what information the asset holds, and what enters and leaves it and</td>
<td>• keeps understanding of the asset and how it is used up to date</td>
</tr>
<tr>
<td>why</td>
<td>• approves and minimises transfers while achieving the business purpose</td>
</tr>
<tr>
<td></td>
<td>• approves arrangements so that sensitive information put onto removable media</td>
</tr>
<tr>
<td></td>
<td>like discs or laptops is minimised and protected</td>
</tr>
<tr>
<td></td>
<td>• approves the disposal mechanisms for paper or electronic records</td>
</tr>
<tr>
<td>Knows who has access and why, and ensures their use of it is monitored</td>
<td>• understands the organisation’s information governance framework</td>
</tr>
<tr>
<td></td>
<td>• check that access provided is the minimum necessary to achieve the business</td>
</tr>
<tr>
<td></td>
<td>purpose</td>
</tr>
<tr>
<td></td>
<td>• receives records of checks on use and assures self that they are being conducted</td>
</tr>
<tr>
<td></td>
<td>• Liaises with team records leads</td>
</tr>
<tr>
<td>Understands and addresses risks to the asset,</td>
<td>• Identifies incidents</td>
</tr>
<tr>
<td></td>
<td>• Monitors training needs and take-up</td>
</tr>
<tr>
<td></td>
<td>• Cascades information to their teams to raise awareness of relevant standards</td>
</tr>
<tr>
<td>Ensures the asset is fully used for the public good,</td>
<td>• considers whether better use of the information could be made</td>
</tr>
<tr>
<td>including responding to requests for access from others</td>
<td>• receives and logs requests from others for access</td>
</tr>
<tr>
<td></td>
<td>• ensures decisions on access are taken accordingly</td>
</tr>
</tbody>
</table>
Appendix 6

Information Governance Steering Group
Terms of Reference

Role and duties
1. The Information Governance Steering Group will oversee operational implementation of the Security Policy Framework and ensure effective information governance and records management standards are applied across NICE.

2. The group will monitor and give effect to information governance and records management policies and ensure these are cascaded to all teams via Information Asset Owners and ensure effective management of sensitive personal data and confidential information.

3. The group will act as a forum for the review and resolution of practical issues associated with information and records management with escalation to the SMT / SIRO / Caldicott Guardian as appropriate.

4. The group will review assurance as to compliance with the Process Manual for the management of HSCIC data approved by SMT.

5. The group will recommend cyber security controls in consultation the IT team and will assist in identifying and managing risks to confidential information within departments.

6. To consider practical actions arising from security incidents that have been agreed by the SMT or Audit & Risk Committee and undertake remedial action.

Membership
7. Core attendees will be:
   a. Director, Business Planning & Resources (chair)
   b. Governance Manager
   c. Associate Director, Corporate Office
   d. Information Asset Owners
   e. Records and Information Manager
   f. Associate Director, Adoption and Impact

8. A quorum shall be three Information Asset Owners plus either the Associate Director, Corporate Office or the Governance Manager.

Meeting frequency
9. The group will meet quarterly. Additional meetings may be held as business requires.
## Appendix A – Version Control Sheet

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Replaces</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>October 2015</td>
<td>Governance Manager</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>