

## Senior Information Risk Owner (SIRO)

The establishment of the role, Senior Information Risk Owner (SIRO) required by the Information Governance Toolkit (IGT) was one of several NHS Information Governance (IG) measures identified to strengthen information assurance controls for NHS information assets. These arrangements are consistent with requirements introduced by Cabinet Office for Departments resulting from the data handling review in Government.

David Nicholson, then Chief Executive of the NHS, in his letter of 20 May 2008 set an action that all NHS organisations also identify a Senior Information Risk Owner and this applies to all organisations completing the IGT and processing NHS patient information.

The nominated person should be an Executive or Senior Manager on the Board who is familiar with information risks and the organisation's response to risk. The role of the SIRO is to take ownership of the organisation's information risk policy, act as an advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk.

The aim is to ensure that the approach to information risk management:

- Takes full advantage of existing authority and responsibility structures where these are fit for this purpose;
- Associates tasks with appropriate management levels;
- Avoids unnecessary impacts on day to day business;
- Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner.

Responsibilities of the SIRO may be in addition to other job responsibilities and to avoid confusion should be identified clearly within the role-holder's job description.

The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by IAOs
- Advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls
- Owning the organisation's information incident management framework

Organisations are required to ensure their appointed SIRO possesses the necessary knowledge and skills to undertake their role effectively and to provide periodic evidenced statements of information assurance to their organisation's accounting officer for the annual Statement of Internal Control. The SIRO should undertake information risk management training at least annually to be able to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation.

The following table describes the functions and responsibilities that are appropriate to all NHS SIROs in greater detail.

**Lead and foster a culture that values, protects and uses information for the success of the organisation and benefit of its customers**

Responsibilities:

- to ensure the Organisation has a plan to achieve and monitor the right NHS IG culture, across the Organisation and with its business partners
- to take visible steps to support and participate in that plan (including completing own training)
- to maintain sufficient knowledge and experience of the organisation's business goals with particular emphasis on the use of and dependency upon internal and external information assets
- to ensure the Organisation has Information Asset Owners (IAOs) who understand their roles and are supported by the information risk management specialists that they need
- to initiate and oversee an information risk awareness / training programme of work to communicate importance and maintain impetus
- to ensure that good information governance assurance practice is shared within the organisation and to learn from good practice developed and practiced within NHS organisations locally and nationally

**Own the organisation's overall information risk policy and risk assessment processes and ensure they are implemented consistently by IAOs.**

Responsibilities:

- to act as the focal point for information risk management in the organisation including resolution of any pan-organisation or other escalated risk issues raised by Information Asset Owners, Information Security Officers, Auditors etc
- to develop and implement an IG Information Risk Policy that is appropriate to all departments of the organisation and their uses of information setting out how compliance will be monitored
- to initiate and oversee a comprehensive programme of work that identifies, prioritises and addresses NHS IG risk and systems' accreditation for all parts of the organisation, with particular regard to information systems that process personal data
- to ensure that Privacy Impact Assessments are carried out on all new projects when required in accordance with the guidance provided by the Information Commissioner
- to review all key information risks of the organisation on a quarterly basis and ensure that mitigation plans are robust
- to ensure that NHS IG Policy, information risk management method and standards are documented, applied and maintained consistently throughout the organisation's information governance risk assessment and management framework
- to ensure that information risk assessment is completed on a quarterly basis taking account of extant NHS Information Governance guidance as required by the IGT.
- to understand the information risks faced by the organisation and its business partners ensuring that they are addressed, and that they inform investment decisions including outsourcing
- to ensure that information risk assessment and mitigating actions taken benefit from an adequate level of independent scrutiny

**Advise the accounting officer on the management of information risk and provide assurance**

Responsibilities:

- to ensure routine meetings are established with the organisation's Chief Executive or Accounting Officer to brief, discuss or report upon matters on information governance risk assurance and information risk culture affecting the organisation, including input to the annual NHS IG reporting processes
- to sign off an annual assessment of performance, including material from the IAOs and specialists, covering NHS Information Governance reporting requirements

### Own the organisation's information incident management framework

#### Responsibilities:

- to ensure that the organisation has implemented an effective information incident management and response capability that supports the sharing of lessons learned
- to ensure that there is a considered and agreed IG incident response and communications plan available, including the reporting of 'perceived' or 'actual' Information Governance Incidents.
- to ensure that the organisation's management, investigation and reporting of IG Incidents conforms to national guidance and does not conflict with the organisation's policies and procedures for non-IG Incidents