Information risk policy

professional standards authority

Document Control

Version Control

Version	Status	Description of Version	Date Completed
1.0	agreed	Information Risk policy	14/11/08
2.0	agreed	Updated to reflect changes in HR policies	08/05/09
2.1	agreed	Changes to titles	03/11/11
2.2	agreed	Changes to reflect CHRE changing to Professional Standards Authority	October 2012
2.3	agreed	Change to section 4.2. to reflect current practice	20/09/2013
2.3		Layout changes	23/02/2016

Contents

1. Purpose

1.1 The purpose of this document is to define how the Processional Standards Authority for Health and Social Care (the Authority) and our delivery partners will manage information risk and how we will assess the effectiveness of our strategies and procedures on managing information risk.

2. Statement of Intent

2.1 Information is a key asset and its proper use is fundamental to the delivery of our services. The public and our other stakeholders are entitled to expect that we will protect their privacy and use and handle information professionally and sensitively to ensure that their private information is protected. We will do this by effectively managing all risks, to the integrity, availability and confidentiality of our information whether held on paper or in our IT systems. Risks include inappropriate disclosure or non-disclosure of information, loss, theft or fraud, information being wrongly destroyed, staff acting in error, and a failure to utilise the information for the public good.

2.2 We see the benefits of managing these risks as being able to:

- ensure that information is being used professionally and in line with all relevant guidance and legislation;
- constrain threats to our information to acceptable levels so that we can maintain public confidence; and
- make informed decisions on when we should share or re-use information so that it can be used to its fullest value.

2.3 We have set down policies and procedures, which will enable the Authority, its employees and its delivery partners to work within an acceptable level of risk, and to be aware of when and whom to contact if they want to deviate from these policies, and the consequences both corporate and individual of not following these procedures.

2.4 The Authority's management team is committed to ensuring that all staff comply with this policy at all times.

3. Information Risk Management Structure

3.1 The Authority has put in place an information risk management structure to ensure that appropriate personnel have responsibility for the management of our information.

3.2 **The Authority's Chief Executive** is the Senior Information Risk Owner (SIRO). He is the focus for the management of information risk at Board level. He is responsible for:

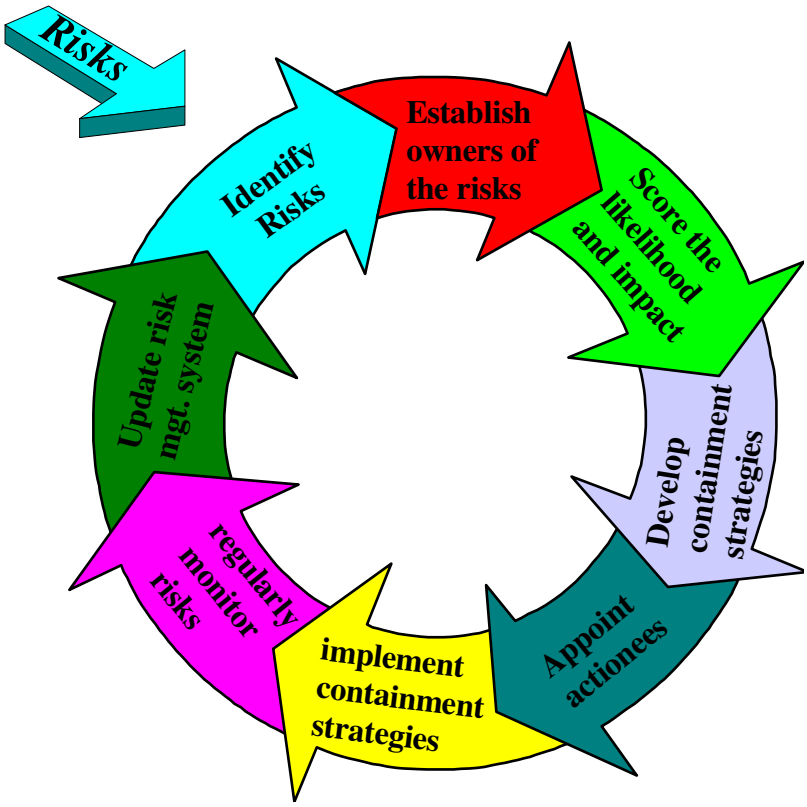
- the overall information risk policy and risk assessment process;
- ensuring that the policies and procedures are implemented, followed and agreeing any deviation from these;
- testing their effectiveness;
- leading and fostering a culture that values, protects and uses information for the public good; and
- reporting to the government on information risk management.

3.3 **The Senior Management Team** are the Information Asset Owners (IAOs). Their role is to understand what information is held, what is added and what is removed from our paper and electronic records, how information is moved and who has access to it and why. As a result, they are able to understand and address the risks to their information, and ensure that information is fully used within the law for the public good. They are also able to provide written input to the SIRO annually on the security and use of their asset.

3.4 **All staff** have the responsibility to manage their information in line with the Authority's record management and information risk policies and procedures. They also have the responsibility to notify the SIRO if there is a breach or a suspected breach of classified and unclassified information.

4. Information Risk Management Strategy

4.1 The risk management process for the Authority is shown below.



4.2 The Governance and Compliance Manager and Information Asset Owners will meet to discuss the risks related to the information we hold internally and that, which is shared or held with our delivery partners, quarterly. We collectively identify risks to our information, agree how to either avoid these, or if that is not possible, to manage the adverse impact of these occurring.

4.3 We pay considerable attention to managing risks and are prepared to take higher organisational risks to improve protection of patients and the public. Managers review risk on an ongoing basis and will tolerate, treat or avoid risks according to the nature of each risk.

5. Threat Assessment

5.1 Our current risk assessment shows that the risks to our information are low. The risks to the information are being managed and this is documented in our risk register. We hold relatively little sensitive personal data and the access rights to this data are limited. We hold a register of staff that have access to these rights and this is regularly reviewed. Staff who have access to this are used to dealing with it appropriately and do so in accordance with our information security policies. Managers also regularly review processes.

6. The Legal and Regulatory Requirements

6.1 When managing our information risk, the Authority works to the required legal and regulatory standards. Whilst this list is not exhaustive, they include:

- The Government's minimum mandatory measures;
- The Data Protection Act 1988;
- The Freedom of Information Act 2000;
- The Authority's record management policies;
- The Authority's policies on protecting personal and sensitive data; and
- The Authority's guidance on reporting, recovering from and managing a breach of information.

7. Building and protecting a culture where we value, protect and use information for public good

7.1 We have a culture where we value, protect and use information for public good. We reiterate regularly to staff the need to ensure that they adhere to The Authority's information governance policies. We have provided staff with information governance training.

8. 'Whistleblowing' policy

8.1 We have a whistleblower policy in place which states that a member of staff will be protected if they raise concerns under this policy about the unauthorised or inappropriate disclosure, misuse or loss of confidential, personal and / or sensitive information.

9. Reporting, Recovering and Managing from an Information breach

9.1 We have a policy in place, which sets out how The Authority will report, recover, and manage an information breach.

10. Corporate and individual consequences of the failure to adhere to information risk policies and procedures

Individual

10.1 We have a dismissal and disciplinary policy and procedure and an IT code of conduct which incorporate the consequences of failing to adhere to the information risk policies and procedures.

Corporate

10.2 There could be significant consequences for The Authority as an organisation if we failed to adhere to our internal information risk policies and procedures. We could face considerable loss of reputation, particularly if there is media interest; we could face action by the Information Commissioner's Office or individuals if personal information was involved; we could face a loss of confidence by our stakeholders; and even a loss of people willing to work with us. Similar consequences could occur to our delivery partners.

11. Inspections

Internal

11.1 We conduct quarterly assessments of the risks to the integrity, availability and confidentiality of our information within our organisation and with our delivery partners. We also complete an annual assessment of information risk management which is recorded in our Annual Report. This is a comprehensive and objective report on the actions that we have taken in the year to manage our information risk, together with any outstanding issues that need to be addressed.

External

11.2 The Authority will comply with any reasonable external requests from the Information Commissioner's Office or others to inspect the implementation of our policies and procedures.