NHS Information Governance:

Information Risk Management

Guidance: Blogging and social networking

Department of Health Informatics Directorate

December 2009

Amendment History

Version	Date	Amendment History
1.0		First published version

Introduction

This Information Governance (IG) guidance provides NHS organisations with a general awareness of the associated risks of blogging and social networking that may potentially affect the effectiveness of local services.

Terms used:

Blogging is using a public website to write an on-line diary (known as a blog) sharing thoughts and opinions on various subjects. The word blog is derived from the phrase weB LOG. Examples of blogging websites include Twitter.com and Blogging.com.

Social networking is the use of interactive web based sites that mimic some of the interactions that occur between people in life. Examples include Facebook.com and Linkedin.com.

Why are Blogging and Social networking an Information Governance issue?

The use of blogging and social networking websites by an NHS organisation's employees can expose that organisation to information risks, even where these sites are not accessed directly from work. Whilst there is nothing new about the information risks, what has changed is the availability of high capacity broadband, the popularity of Web2.0 sites and the rapid growth of internet enabled devices such as mobile phones, blackberries etc. This has resulted in significant awareness and uptake of these websites from home, from work and when mobile.

What are the potential dangers to the organisation of using blogging and social networking?

A range of potential threats exist that organisations should be aware of:

- Unauthorised disclosure of business information and potential confidentiality breach

  Blogging and social networking sites provide an easy means for information to leak from an organisation, either maliciously or otherwise. Once loaded to a site, organisational information enters the public domain and may be processed and stored anywhere globally. In short, organisational control is lost and reputational damage can occur.

- Malicious attack associated with identity theft

  People often place a large amount of personal information on social networking sites, including details about their nationality, ethnic origin, religion, addresses, date of birth, telephone contact numbers and interests. This information may be of use to criminals who are seeking to steal identities or who may use the information for social engineering purposes.

- Legal liabilities from defamatory postings by employees

  When a user registers with a site they typically have to indicate their acceptance of the site's terms and conditions. These can be several pages long and contain difficult to read legal language. Such terms and conditions may give the site 'ownership' and 'third party disclosure' rights over content placed on the site, and could create possible liabilities for organisations that allow their employees to use them. For example, where a user is registering on a site from a PC within the organisation, it may be assumed that the user is acting on behalf of the organisation and any libellous or derogatory comments may result in legal action. In addition, information being hosted by the website may be subject to other legal jurisdiction overseas and may be very difficult to correct or remove.

- Reputational damage

  Ill considered or unjustified comments left on sites may adversely affect public opinion toward an individual or organisation. This can lead to a change in social or business status with a danger of consequential impacts.

- Malicious code targeting social networking users causing virus infections and consequential damage

  Sites may encourage or require the download and installation of additional code in order to maximise the site's functionality and potential values. Where sites have weak or ineffective security controls it may be possible for code to be changed to contain malicious content such as Viruses and Trojans, or to trigger unintended actions such as Phishing.

- Systems overload from heavy use of sites with implications of degraded services and non-productive activities

  Sites can pose threats to an organisation's information infrastructure. Particularly as the use of rich media (such as video and audio) becomes the norm in such sites, the bandwidth consumption generated by these sites can be significant and they have the potential to be the biggest bandwidth consumers within an organisation.

- Intimidation of employees from inappropriate use of sites leading to investigations

How might the organisation respond to these risks?

Whilst there are technical controls that could be applied the main defence against threats associated with blogging and social networking is awareness related.

Actions that may be considered by NHS organisations include:

- Deploying technical controls to block or control permitted website usage;

- Revising and updating organisational policies to include acceptable use of blogging and social networking sites. Policies and standards should be clear about the acceptability of accessing sites during working hours and from the organisation's internet connected devices eg. PCs, mobile phones etc. The consequences of non-compliance with organisational policy should also be clear;

- Educating users about the potential business risks and impacts associated with blogging and social networking. Raising user awareness is an essential partner to the organisation's policy and standards and should ensure that the potential dangers are known to employees who may use such sites. This will also help employees in their safe use of such services when at home.

Avoiding problems with blogging and social networking sites

A number of checks may be applied that will help NHS organisations and their employees avoid problems:

1. Verify if the organisation has a relevant policy and the extent to which this applies

2. Ensure that Social Networking and Blogging risks are considered within the overall approach to information risk assessment and management

3. When registering with a website, understand what you are signing up to and importantly what security and confidentially claims and undertakings exist

4. Watch for add-ons i.e. additional features or applications that change the terms and conditions of what you have signed up for, or that may require changes to the security settings of your devices

5. Withhold personal details that you do not want to be made public

6. Avoid loading work related information to blogging or social networking sites

7. Examine carefully any email coming from social networking sites or contacts as these may be unreliable containing malicious code or be spoofed to look as though they are authentic