NHS Information Governance:

Information Risk Management

Guidance:

Social Interaction – Good Practice

Department of Health Informatics Directorate

February 2012

Amendment History

Version	Date	Amendment History
1.0		First published version

Introduction

NHS organisations of all types are now making increased use of Social Networks to engage with their patients, other stakeholders, and to deliver key messages for good healthcare and patient services generally. These online digital interactions are encouraged and their uses likely to be further extended as new communications channels become available.

This Information Governance (IG) guidance provides NHS organisations and their staff with general awareness of the information risks and good practices associated with the protection of sensitive information in social media and other social interaction scenarios.

The terms often used in this context sound very similar and can therefore be potentially confusing. Explanations of these terms and their different meanings are provided below to aid reader understanding.

This guidance replaces and extends the NHS IG Guidance previously provided for Blogging & Social Networking published in December 2009.

Terms used:

Social Media is the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others who often share the same community interests. Such technologies can include blackberry messaging, instant messaging and other similar services etc.

Social Networking is the use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook, Bebo, Myspace and Linkedin.

Social Engineering is the method whereby an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation’s staff or maintenance contractor etc.

Blagging is the term commonly used to describe the deliberate, reckless and potentially criminal obtaining and/or disclosing of personal information about individuals without that person’s knowledge or valid consent. Recent media reports allege that blagging is an issue that may particularly affect individuals who are of media interest but may potentially affect anyone.

The terms Social Engineering and Blagging are sometimes used interchangeably to describe methods of hacking into systems including phone services or where trickery is used to fool people into disclosing confidential information.

Guidance is provided below in order to help clarify these issues for NHS organisations and their staff.

Blogging or Tweeting (micro-blogging) is using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video. Many blogs and tweets are interactive allowing visitors to respond leaving comments or to potentially send messages to others. It is increasingly common for blogs to feature advertisments to financially benefit the blogger or to promote a blogger’s favourite cause. The word blog is derived from the phrase weB LOG. Examples of these websites include Twitter.com and Blogging.com.

Social Networking and Blogging

Why are Social Networking and Blogging an Information Governance issue?

The use of blogging and other social networking websites by an NHS organisation's staff can expose that organisation to unexpected information risks or liabilities, even where these social media 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 mobile devices such as iPads, Tablets, smart phones, BlackBerrys etc. This has resulted in significant awareness and uptake of these websites from home, from work and when roaming.

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

A range of potential risks and impact consequences exist that NHS organisations should be aware of:

- Unauthorised disclosure of business information and potential confidentiality breach

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

- Malicious attack associated with identity theft

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

- Legal liabilities from defamatory postings etc by staff

  When a person registers with a website 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 and understand legal jargon. Such terms and conditions may potentially 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 staff member is registering on a website from a PC within the organisation, it may potentially be assumed that the user is acting on behalf of the organisation and any libellous, inflammatory or derogatory comments may result in civil litigation or criminal prosecution. 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 and professional opinion toward an individual, their employer or another implicated organisation, contractor, service provider or business partner etc. This can lead to a change in social or business status with a danger of adverse consequential impacts and possibility of legal proceedings.

- Malicious code targeting social networking users causing virus infections and consequential damage to end user devices

  Sites may encourage or require the download and installation of additional code in order to maximise the site's functionality and potential values. Where such sites have weak or ineffective security controls it may be possible for its operating system or application code to be changed to contain malicious content such as Viruses and Trojans, or to trigger unintended actions such as Phishing – a way of obtaining sensitive information through bogus impersonation as a trustworthy entity.

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

  Sites can pose threats to an organisation's own information infrastructure. Particularly as the use of rich media (such as video and audio) becomes the norm in such sites, the network bandwidth consumption generated by these sites can be significant and they have the potential to be the biggest bandwidth consumers within an organisation. In an aggregated sense widespread use of blogging and social networking sites may introduce new capacity issues for local and national NHS infrastructure and services.

- Staff intimidation or harassment with the possibility of personal threat or attack against the blogger, sometimes without apparent reason.

  Other online bloggers can hold strong views and may potentially be offended at what they read, however unlikely or unintended that might seem. In extreme cases this negative reaction could lead to targeted attack or assault against the original blogger with potential to cause them anxiety, distress and personal safety issues.

How might the organisation respond to these risks?

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

Actions that should be considered by NHS organisations include:

- Deploying technical controls to block or manage locally permitted website usage;

- Revising and updating organisational policies to include terms and conditions for use of blogging and social networking sites, including any requirements that may apply to staff who leave the organisation. 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, smart phones etc. The consequences of non-compliance with organisational policy should also be clear. (See Annex A);

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

- Consider having separate official email addresses for social networking to avoid giving out unnecessary contact details.

- Provide corporate policies for staff who use and publish attributed official digital content eg. Digital Communication at the Department of Health:

  http://digitalhealth.dh.gov.uk/

  http://digitalhealth.dh.gov.uk/official-attributed-content-policy/

Staff guidance - Avoiding problems with blogging and social networking sites:

Good Practice Tips:

1. Check that your organisation has a relevant policy and know the extent to which this applies to your use of Social Networking or Blogging websites;

2. Ensure that the Social Networking and Blogging risks possible are considered within your organisation's overall approach to its IG information risk assessment and management. If in doubt seek advice from your local IG team;

3. When registering with a website, understand what you are signing up to by reading the terms and conditions carefully and importantly determine what security, confidentially and liability claims, undertakings and exclusions exist. If in any doubt seek the advice of your local IG team;

4. Be careful about the personal details you post online;

5. Think about what you want to use your online profile for, applying appropriate security and preferences settings as necessary;

6. Keep your password safe and avoid obvious ones that others might easily guess;

7. Be aware of your personal responsibility for the words you post and also for the comments of others you allow on your blog or webpage. Don't say anything on-line that you would not say personally or wish others to hear. Avoid unattributable anonymous comments.

Social Engineering and Blagging

Why are Social Engineering and Blagging an Information Governance issue?

All NHS organisations collect, process and store vast quantities of information of all types including clinical and other potentially sensitive information about their patients, staff members and other third parties with whom the organisation interacts. Whilst all NHS organisations will have existing strong cultures of confidentiality, it is possible that targeted attacks may occur where information is known or suspected to exist about a patient or member of staff of particular interest.

In such cases, the techniques of Social Engineering and Blagging may be attempted to gain access to private or confidential information. In this regard there are a range of possible motivations a Social Engineer or Blagger may have and it is equally possible for multiple attackers operating together to gain and combine pieces of information about the organisation that may then be used against it.

How big an issue is this?

Social Engineering and Blagging account for a large percentage of known information breach attempts and successes. Criminals, fraudsters and other tricksters are always on the lookout for valuable information and will look for new and innovative ways to access and obtain this type of information. NHS organisations are not immune to such attacks and it is possible for all departments of the organisation and their staff to be subject to probing. This can be through seemingly innocent face to face conversation, telephone calls, email, faxes, letters that look convincing etc. In short, it is an issue that could affect anyone.

What can the organisation do to avoid becoming a victim?

Acknowledging the possibility of such an attack is key to understanding how corporate risks and safeguards might apply. Departments should encourage their staff and contractors to consider if and how their role may be of interest to a potential attacker. This will include an understanding of the information they have access to, its sensitivities, its protection needs, and what values it may have to others.

Other actions possible by the organisation will include:

- Educating staff about the potential business risks and impacts associated with Blagging and Social Engineering. Raising user awareness is an essential partner to the organisation's policy and standards and should ensure that the potential risks are known to employees and others who may be vulnerable to such attacks.

  https://www.igte-learning.connectingforhealth.nhs.uk/igte/

- Ensure your organisation has implemented up to date security software eg. anti-virus, spam email filters and firewall to ensure that as far as possible potentially malicious network communications are blocked and phishing email discarded.

In addition to the above points, NHS organisations should ensure their local information risk assessments are regularly refreshed to take account any new information assets and changes to existing ones. This approach will ensure:

- Local security policies and countermeasures remain effective;

- Staff and contractor training needs and methods are updated;

- Audit and assurance mechanisms remain appropriate

Staff guidance – Recognising and addressing potential problems:

Good Practice Tips:

- Be suspicious of all unsolicited contacts. This can include phone calls, visits, faxed messages, email, SMS messages etc from anyone asking about information about other staff, contractors and patients or other potentially confidential information;

- Where a new contact claims to be a legitimate member of staff or a business partner organisation etc ensure you take steps to verify their identity and business needs directly with their department head or other organisation;

- Do not provide information about your organisation, its patients or other individuals including structures and networks unless you are certain of the recipient's identity and authority to have that information. Check that the intended recipient has appropriate IG arrangements in-place to handle any information disclosed to them;

- Avoid disclosing personal or other sensitive information in email. Where this is necessary ensure the recipients email address is verified and legitimate, and that appropriate data encryption standards are used for patient and other sensitive information. Using the NHS strategic NHSMail messaging system ensures that all email and their contents are encrypted in transmission by default between NHSMail users;

- Don't send personal or other sensitive information over the Internet unless you are completely confident in the website's implemented security and its legitimacy. The URL or address of a website may at first glance look convincing and legitimate but could contain spelling errors or other variation eg. '.co.uk' / '.org.uk. 'Secure' sites often have a 'http**s**' prefix in their web address, and a padlock icon in the browser (where the browser supports this). The presence of these items may provide additional confidence that the site in question is legitimate and not a 'spoof' or cleverly designed copy, intended to fool those who may overlook such detail;

- In the event that you think you may have been a social engineering or blagging victim ensure you immediately report this as an incident in accordance with your organisation's IG incident policy. Additional advice will be available from your IG team where necessary. It is possible that a notice may be issued to other staff within the organisation with appropriate guidance to be alert to any new, unusual or suspicious activity.

Annex A

[The Organisation]: Social Media Policy

Draft only - provided for illustration purposes

Introduction:

This policy is provided so that staff and contractors (of the organisation) are aware of their personal responsibilities for appropriate use of social media facilities they may access. Within the policy scope are the uses of both NHS and other external websites and online blogging facilities.

The policy is necessary as many employees and contractors enjoy sharing their knowledge and experience with others of similar roles and interests. (The organisation) encourages these online activities and acknowledges that staff and contractors can improve their personal skills and experience through relevant interactions with others outside the organisation. However, (the organisation) has responsibility to ensure the operational effectiveness of its business, including its public image, reputation and for the protection of its information assets of all kinds. This involves ensuring confidentiality and maintaining security in accordance with NHS Information Governance policy and good practice.

Staff and contractors whose role for (the organisation) includes establishing, contributing to and maintaining official blogs and websites are guided through their individual job descriptions and related work instructions.

Private use of Social Media:

Staff and contractors (of the organisation) may use designated facilities provided (by the organisation) for their private Social Media purposes during their work breaks. They are encouraged not to divulge who their employers are within their personal profile page (eg. in accordance with RCN guidelines, “RCN Legal Advice on using the internet”), However, those that do divulge their employer should state that they are tweeting/blogging etc. in a personal capacity. The use of other non-designated facilities for private purposes is prohibited.

Staff and contractors (of the organisation) are ultimately responsible for their own online behaviour. Staff and contractors must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassment, threatening or may otherwise be illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution.

Staff and contractors are not authorised to communicate by any means on behalf of (the organisation) unless this is an accepted normal part of their job, or through special arrangements that have been approved in advance (this may be facilitated through an Official Attributed Content Policy).

Sensitive and Confidential Information:

Staff and contractors who use Social Media must not disclose information of (the organisation) that is or may be sensitive or confidential, or that is subject to a non-disclosure contract or agreement. This applies to information about patients, other staff and contractors, other organisations, commercial suppliers and other information about (the organisation) and its business activities.

Corporate logos or other visible markings or identifications associated with (the organisation) may only be used where prior permission has been obtained.

Information Security:

Staff and contractors must not share details (of the organisation's) implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security occurring.