

**NHS Information Governance:
Information Risk Management**

Guidance: Dealing with Cookies and Legal Compliance

Department of Health Informatics Directorate

January 2012

Amendment History

Version	Date	Amendment History
1.0		First published version

Introduction

This Information Governance (IG) guidance provides NHS organisations with general awareness of the issues affecting the use of Cookies in websites that target UK users. It builds upon the introductory Information Governance Toolkit (IGT) news item published on 17th May 2011.

Please see: [Changes to the rules on using cookies and similar technologies for storing information](#)

Terms used:

Cookies are small computer files, typically containing letters and numbers that are created through web browsers. Cookies are used as a form of digital memory to remember bits of information about a user's visits to and use of web pages. They are mostly intended to enhance the user's web experience by recording preferences and settings. However, Cookies can also be used as 'trackers' to collect data about web sites and pages visited. This information may then be used to display web content and advertisements thought to be of most interest to the individual concerned.

For more information see: <http://www.allaboutcookies.org>

Why are Cookies an Information Governance issue?

On 26th May 2011 a new EU privacy law came into effect that requires website owners of all kinds to review their website uses of Cookies and where necessary implement improvements that enable compliance. This legislation requires the informed consent of website visitors before cookie data may be collected and stored. By requiring website owners to inform web users and obtain explicit consent for cookies the law aims to give web users greater control over their on-line privacy.

Within the UK, the government has updated the Privacy and Electronic Communications Regulations (PECR) giving website owners until 25th May 2012 to comply. A helpful summary has been provided by The Information Commissioner:

http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications.aspx

What should be done to minimise the IG risks and ensure legal compliance?

It is essential that NHS organisations should always undertake, document, review and maintain a statement of their deployment and use of Cookies within their planned or existing websites including:

- An assessment of what cookies (Session or Persistent, First Party and Third Party) are to be deployed and what information will be collected;
- How that information will be used;
- What choices will exist for website users including issues of consent;
- What new or updated web user explanations, website publicity or guidance will be necessary.
- How cookie compliance audit and assurance will be achieved

Avoiding compliance problems through risk treatment

The Information Commissioner's Office is charged with regulating the new rules for websites that target UK consumers. In cases where an organisation refuses or fails to comply voluntarily the Information Commissioner has a range of options available to take formal action where this is deemed necessary. These options include Information notices, undertakings, enforcement notices and monetary penalty notices up to a maximum of £500,000.

In enforcing the rules on cookies, the Information Commissioner has provided a 12 month lead-in period to allow website owners time to assess and address cookie compliance. At the end of this period in May 2012 the Information Commissioner will consider complaints about cookies in line with established arrangements for complaint handling. Further detail about the Information Commissioner's role, responsibility and powers is provided below.

Please note that the NHS IG helpdesk is unable to provide support to NHS website owners concerning cookie identification, compliance requirements or cookie treatment for their websites. Local Senior Information Risk Owners, Information Asset Owners, IT Managers and where appropriate their external website providers must consider the latest available guidance and good practice when assessing and addressing their local compliance needs.

Information Commissioners Office

A **half-term assessment report** has now been published along with new updated '**Guidance on the rules on use of cookies and similar technologies**'. These contain detailed guidance including information concerning the meaning of consent, the purposes for which cookies are used, conducting a cookie audit and other helpful examples. The documents are available to download via the provided ICO website links:

<http://www.ico.gov.uk/news/blog/2011/half-term-report-on-cookies-compliance.aspx>

http://www.ico.gov.uk/news/latest_news/2011/~media/documents/library/Privacy_and_electronic/Practical_application/guidance_on_the_new_cookies_regulations.ashx

Additional Illustration of a website providing information about Privacy and Cookies:

The following internet web links relate to a major UK non-NHS organisation. **Please note** external website links are provided for additional illustration purposes only. It is possible that the website owner may introduce further changes and content should not be interpreted as representing NHS IG Policy.

BBC website

- Protecting your privacy - <http://www.bbc.co.uk/privacy/>
- BBC Cookies - <http://www.bbc.co.uk/privacy/bbc-cookies-policy.shtml>

In addition the BBC has published a Blog that outlines its strategy to comply with UK Cookie law changes:

- http://www.bbc.co.uk/blogs/bbcinternet/2011/05/cookie_laws_changes.html