

Reference: RJT/MG/lmd



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Mr Hugh Taylor CB
Permanent Secretary
Department of Health
334B Skipton House
80 London Road
London
SE1 6LH

5 May 2009

Dear Hugh,

You will probably be aware that my office has been collecting information on self reported security breaches since November 2007. I am concerned at the number of breach notifications involving personal data made by organisations that fall within the remit of the Department of Health (DOH) and I wish to bring to your attention the volume and nature of these. The breach reports have been notified to us by primary care trusts, hospitals and GP surgeries. Most of the reported breaches relate to patient information held electronically or in paper form which has been lost or stolen. Most of the information is 'sensitive' personal data as defined by Section 2 of the Data Protection Act 1998 (the Act). This personal information has the potential to cause significant distress and, in some cases, damage to individuals if compromised.

A breach in this context means a breach of the seventh data protection principle in Schedule 1 of the Act which addresses security. There is often an associated breach of the third data protection principle where the information used is excessive for the purpose for which it is being processed. In the period from the end of November 2007 to the 31 March 2009 we have been notified of 434 self reported security breaches involving personal data. Of these 115 involved NHS organisations the majority of which fall within the remit of the DOH.

Our Regulatory Action Division examines all reported security breach notifications and we have now taken regulatory action against three primary care trusts, five hospitals and an individual general practitioner. There are other breach notifications currently under investigation which are likely to result in further regulatory action against NHS organisations. Many of the security breaches listed above occurred as

.../



RJT/MG/lmd
Mr Hugh Taylor CB
5 May 2009

a result of poor internal governance, for example, where organisations have inadequate or non-existent procedures and policies in respect of data security. There is also little evidence of effective staff training taking place in some areas of data security.

There are clear risks associated with personal data which is held electronically and not adequately protected. The portability and increased capacity of laptop computers and USB memory sticks can and does give rise to poor data handling practices. Furthermore, the increased use of portable media devices in home and office computers raises the risk of viruses being imported.

In our experience security breaches are often associated with, portable media devices being used by employees to download personal information to work with in other locations. In such circumstances data minimisation does not always seem to be considered. When the information is not encrypted this information in my view becomes a 'toxic liability.' There is a ready market for portable storage devices such as laptop computers and USB memory sticks which clearly attracts the attention of opportunist thieves. An additional problem is that the organisation concerned is often unaware that information has been downloaded even though such action may be against local policies.

The effects of the loss or theft of electronic media can though be mitigated by the implementation of data encryption and computer port control. I welcome the DOH guidance in this area and the resources that have been made available to implement it. I also welcome the fact that many organisations in the health sector are now implementing these measures. Unfortunately there is evidence that some organisations are reluctant to do so despite being offered the necessary resources.

I should therefore be grateful if you could provide me with an indication of the current extent of the implementation of encryption and port control measures together with an idea of when the roll out will be complete. It would also be helpful to know what action the DOH is likely to take against those organisations in the public health sector that fail to introduce adequate encryption and port control measures.

.../



Information Commissioner's Office

-2-

RJT/MG/lmd
Mr Hugh Taylor CB
5 May 2009

I am confident that with your assistance the number of data security breaches can be reduced, and along with this, the need for formal enforcement action by my office. I should therefore be grateful if, in responding to this letter, you could provide me with an outline of any additional steps the DOH will be taking to address the issues of data security affecting organisations within its remit.

Yours sincerely
A handwritten signature in black ink, appearing to read 'Richard Thomas', written in a cursive style. The signature is positioned below the text 'Yours sincerely'.

Richard Thomas
Information Commissioner