

● Medico-legal advice

Patient information and data protection



Madeleine Delaney, Beauchamps Solicitors, looks at the Data Protection Commissioner's recommendations to the HSE to increase security of patient information

The Data Protection Commissioner (the Commissioner) called on the Health Service Executive (HSE) to increase security of patient information in his 2009 annual report which was published on 8 April 2010.

On 31 May 2010 the Commissioner also published a draft Data Security Breach Code of Practice for public consultation in response to a recommendation in the recent report of the Data Protection Review Group and public concern about recent data losses. It will set out the circumstances in which disclosure of data breaches is mandatory.

Failure to comply with the disclosure obligations of the Code could lead to prosecution by the Commissioner.

What is data protection?

The purpose of the Data Protection Acts 1988 and 2003 (the Acts) is to protect the privacy of individuals in respect



of personal data such as personal health information which are held in a processable form, through the regulation of data controllers and data processors that collect, process, keep or use such data. Data includes both 'automated data' and 'manual data'. Therefore when personal details are given to

an organisation or individual, they have a duty to keep them private and safe. In the context of medical records the data controller could be the HSE, a hospital, a clinic or a GP.

HSE laptop theft

The Commissioner's request that the HSE increase pa-

tient information security was sparked by the investigation resulting from a robbery at the HSE West Primary, Community and Continuing Care 4 offices in Roscommon in June 2009 in which an unencrypted laptop containing personal data related to HSE clients was stolen.

The investigation by the Commissioner concluded that the HSE failed to have security measures on the stolen laptop that were appropriate to the harm that could result to individuals from the loss of the data.

More specifically the Commissioner called for the HSE to:

1. Take organisational responsibility for the encryption of all laptops; it is not sufficient to delegate this responsibility to individual staff members. All HSE areas should make arrangements with their laptop suppliers to ensure that laptops are en-

rypted before they are allocated to staff members.

2. Introduce policies to prevent similar situations arising in which they do not own or control devices storing HSE patient data.
3. Prioritise the development of secure networks and devices for the transfer of patient data.
4. Train staff to recognise when the creation of a record amounts to a new database and to understand the nature of the controls around such developments. The investigation found that the existing controls on patient database development within the HSE are insufficient to prevent the development of ad-hoc databases.
5. Develop appropriate controls governing access to patient databases, including directory services.
6. Improve staff training to ensure that all staff, particularly at management level, understand the need to report serious data security breaches. The HSE should develop a comprehensive breach management policy to cover all forms of data security breach including those involving manual data.

to the HSE are in line with the provisions of the Acts and his efforts to encourage public and private sector bodies to voluntarily report personal data security breaches to his office. He states in his report that he will be following up with the HSE to ensure it progresses the above.

Under the Acts, appropriate security measures must be taken against unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to the data. In determining appropriate security measures a data controller such as the HSE must have regard to the nature of the data concerned and the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to the data.

The Acts also provide that an organisation should take all reasonable steps to ensure that its staff and other persons at the place of work concerned are made aware of the security measures and comply with them.

● Madeleine Delaney,

Associate,
Beauchamps Solicitors
Email:
m.delaney@beauchamps.ie

● Neuroscience