Redacción Médica
" Periódico crítico y defensor de los intereses morales y materiales de los profesores de las ciencias del curar" (El Látigo Médico, 1859)
Una publicación de SANITARIA 2000
13 de mayo de 2010
Hemeroteca

ECOS Y COMENTARIOS

Ricardo de Lorenzo

Actualización: 13/05/2010 - 10:13H

LA RELACIÓN MÉDICO-PACIENTE Y LA SEGURIDAD DE LOS DATOS

Uno de los mayores riesgos a los que los centros sanitarios se enfrentan con la implantación de las nuevas tecnologías y la gestión de los datos sanitarios en formato electrónico es la salida no autorizada de información.

El centro sanitario debe poner los medios necesarios para asegurar la integridad de la información, y para evitar pérdidas y accesos indebidos, no sólo por ser una de las obligaciones que la Ley Orgánica de Protección de Datos dispone, sino por el daño que un acto de este tipo puede provocar en la imagen de un Hospital o una clínica, afectando directamente a la calidad asistencial prestada. Sin embargo, en la mayoría de los casos, cuando se produce una pérdida de datos no se debe a una actuación maliciosa por parte de los trabajadores, sino a la falta de concienciación de los riesgos que puede conllevar sacar información del centro.

Por este motivo, los hospitales deben invertir en formación para sus trabajadores, para que conozcan los riesgos que una acción a la que ya estamos tan habituados como puede ser utilizar el correo electrónico o grabar información en un pen drive, puede conllevar cuando se adjuntan datos de salud de pacientes. En estos casos el tamaño es proporcional al riesgo de pérdida, cuanto más pequeño sea el soporte que contiene la información, más probable será su pérdida accidental.

Los centros deberían tener una política de seguridad respecto de la posibilidad de sacar información. Así, sólo el personal que para el desarrollo de sus funciones necesite trabajar con información fuera del centro, podrá ser autorizado. En casos puntuales, deberá existir un registro en el que el responsable autorice al trabajador a sacar la información fuera del centro sanitario.

En segundo lugar, para asegurar la fiabilidad de los soportes es el centro quien debe ponerlos a disposición de sus trabajadores, así éstos cumplirán con unos requisitos mínimos de seguridad, como permitir el cifrado de los datos y verificar el correcto funcionamiento de los mismos, que garantice la integridad de los datos que se copian.

Una vez garantizada la fiabilidad del soporte y habiendo restringido al personal autorizado para grabar datos y sacarlos fuera del centro de trabajo, se está limitando la posibilidad de que ocurra cualquier incidencia. No obstante, es muy importante concienciar a los usuarios de estos soportes que cuando la documentación incluya datos de pacientes se debe cifrar el contenido de los mismos, o al menos establecer contraseñas que dificulten la lectura de los documentos puesto que de esta manera ante la posible pérdida del dispositivo, en principio, evitaríamos que el contenido fuese accesible por personas no autorizadas.

Se debería informar asimismo a los trabajadores de qué deben hacer con la documentación que han sacado del centro, ya que no sería correcto que la grabaran en sus ordenadores personales puesto que se estarían tratando datos de carácter personal sin las medidas de seguridad adecuadas. Una vez que ese fichero temporal ha perdido su utilidad debe ser borrado o destruido.

Así las cosas, se deberían tener en cuenta todos los aspectos referentes a la seguridad, puesto que, independientemente de las sanciones económicas que la Agencia puede imponer ante su inobservancia, de cara a los pacientes, noticias como la pérdida de documentación o los accesos indebidos debilitan la relación médico – paciente que debe basarse en la garantía más absoluta de la confidencialidad de los datos.