WINSTON & STRAWN LLP

BLOG

U.K. ICO Fines Health Agency $498,300 for Data Security Failures

JUNE 21, 2012

The Brighton and Sussex University Hospitals NHS Trust, located in southern England, recently agreed to pay the U.K. Information Commissioner's Office (ICO) a total of €325,000 ($498,300) in civil penalties to resolve a data breach incident. The issue came to light after the Trust discovered that four Trust hard drives had been sold to a third party online. These drives had been slated for destruction by the Trust, which had hired a third-party vendor to destroy them in a group of 1000 hard drives. The four drives included highly sensitive personal information, including medical conditions, sexual preferences, STD test results, National Insurance numbers, addresses, and information about criminal convictions and suspected offenses. The Trust voluntarily notified the ICO following recommended procedures for responding to data breaches set forth by the ICO. Upon notification the ICO conducted an investigation, and as a result of that investigation, discovered 15 more hard drives that were sold that contained sensitive information. The ICO found that by selecting a vendor that did not provide adequate safeguards, the Trust had violated the UK Data Protection Act, which requires, *inter alia*, taking reasonable steps to prevent accidental loss, and selecting a third party vendor that will provide sufficient security guarantees. According to the ICO, the Trust should have ensured that logs of destroyed hard drives were maintained, should have identified the risks of a breach sooner to mitigate the damage to patients and staff, and should have maintained better supervision over the vendor and its employees. The ICO indicated that by making a voluntarily notification, lower penalties were assessed.

Tip: When developing a data breach notification plan, keep in mind that other jurisdictions may have voluntary reporting to state authorities that if followed, can help lower potential fines. To avoid the need to make such notifications, look not only at security measures you have in place for your own employees to follow, but also the security requirements and controls you impose on vendors.

1 Min Read

Related Topics

Europe Privacy | Data Breach | Health Care Privacy

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.