

Will We Ever Learn?

Written by **Mike Davis**
Senior Research Analyst
Butler Group



The announcement that the confidentiality of 185,000 medical records had been potentially compromised, after two Dell personal computers belonging to the San Jose Medical Group in California, US, were stolen, beggars belief. Not because the computers were stolen – that is a perennial risk, which even the IT equipment of the security services cannot avoid – but because there was no need for the information to be on the machines in the first place, and any information that was stored should have been made inaccessible to persons not authorised to see it.

The Big Picture

The Medical Group had apparently copied the data, which included patient medical details along with financial data, from its servers in order to undertake a billing project. Unfortunately only part of the data was encrypted.

The simple fact is that good practice states that ALL of the information should have been anonymised for the project. Research ethics in medicine dictates that patient information should be anonymised. Why is a financial project apparently exempt from this?

The records should never have left the central, secure repository. The Medical Group has stated that whilst the records were on the servers, employees could only access them via a secure network. This statement does not mitigate what occurred, nor does it explain why the records 'needed' to be copied to personal computers for the project.

Document and Records Management (DRM) technologies are not rocket science. They are mature and, if implemented correctly, would allow copies of data sets to be created on the secure repository, which could then be anonymised for use in the project. During transmission, and if there was any requirement for local storage, the data should have been encrypted by default.

Despite this incident being related in an IT publication, the problem is not one of technology, it is one of management and the implementation of policy.

During my time as a manager in the UK National Health Service, on more occasions than I care to remember, I found patient records just left on counters to which the public had access or even on full display in the back of cars. Electronic records by their very form are less accessible than their paper equivalents, but once accessed, they can be just as vulnerable to unauthorised publication, manipulation, or deletion, unless they are secured.

Another worrying aspect of this case is that it took nine days for the Medical Group to identify the 185,000 individuals whose records had been potentially compromised. Again any decent DRM system would have recorded information that was transferred.

Butler Group Opinion

This should never happen again – but unfortunately it will.