

# NHS Surrey fined £200,000 after losing patients' records

The NHS Surrey data breach was one of the most serious the ICO has seen.

NHS Surrey has been fined £200,000 by data regulators over the loss of sensitive information about more than 3,000 patients.

Thousands of children's patient records were found on a second-hand NHS computer that was auctioned on eBay, the BBC understands.

Regulators said NHS Surrey failed to check that a data destruction company had properly disposed of the records.

Three further computers that had been sold on eBay contained sensitive data.

UK watchdog the Information Commissioner's Office (ICO) imposed the fine on the trust after patients across Surrey were affected by the data loss.

"The facts of this breach are truly shocking," ICO head of enforcement Stephen Eckersley said in a statement.

"NHS Surrey chose to leave an approved provider and handed over thousands of patients' details to a company without checking that the information had been securely deleted.

"The result was that patients' information was effectively being sold online."

A Department of Health spokesperson said: "We take the loss of personal data very seriously.

"At the time NHS Surrey contacted patients involved to make them aware of the data breach.

"This case is currently the subject of legal proceedings."

## Free deal

The breach was one of the most serious that the ICO had seen, the data watchdog added.

NHS Surrey was alerted to the data loss by a member of the public who had purchased an old NHS computer and found patient records.

Upon investigation, the trust discovered the computer contained the health records of 2,000 children and 900 adults, plus a number of NHS human resources records.

A further 39 computers that had been sold by the data destruction company were recovered during the course of the investigation, with sensitive records found on three of the hard disks.

The data destruction company had offered free disposal of the computers in exchange for the sale of salvageable materials.

The company promised to crush the computer hard disks using an industrial guillotine, but NHS Surrey failed to monitor the destruction process, the ICO ruled, and did not have a contract in place that explained the legal requirements of the data destruction.

NHS Surrey was decommissioned in March following health service reforms. Responsibility for the fine now rests with the NHS Commissioning Board, which must appeal by 19 July, or pay by 22 July.

The ICO has imposed a number of fines on NHS bodies for data breaches, including a record £325,000 fine after a theft from a Brighton hospital trust in June 2012.

