Omnicell Media Statement

Throughout our 20-year history, Omnicell has been committed to ensuring that patients receive medications and supplies in the most safe and secure manner possible. On November 14, 2012 an Omnicell laptop containing medication dispensing cabinet log files from three health system customers was stolen from an Omnicell employee's locked vehicle.

The files contained data which included patient names, admissions records data, and technical data about medication dispensing transactions from our medication dispensing cabinets over a one to three-week period, downloaded by the employee while troubleshooting software for the hospitals.

The information, stored in engineering log files on the device, included data about the affected patient's medication dispensing transactions from Omnicell medication dispensing cabinets. The device did not include any addresses, phone numbers, credit card, debit card, or bank account numbers of any patients. Further, the patients' general medical records were not on the laptop and are not at risk.

Upon learning of the theft of the device and the involvement of electronic protected health information, we promptly notified each affected Omnicell customer. These three health systems are now in the process of notifying their involved patients. In addition, we are working to ensure these customers experience as little disruption as possible in their delivery of quality medical care.

We do not know of any prior breach of protected health information to have occurred at Omnicell. This was an isolated incident in violation of existing company policies. Omnicell takes very seriously the privacy and security of personal health information, and we have initiated immediate and definitive measures to prevent a similar incident from re-occurring.