For immediate release

U-M Health System notifies patients of vendor incident that led to data breach

ANN ARBOR, Mich. — The University of Michigan Health System is notifying approximately 4,000 patients about an incident that may have exposed some of their health information.

UMHS was notified on Nov. 20 by one of its vendors, Omnicell, that Omnicell electronic equipment containing some UMHS patient medication information – as well as patient information for two other hospitals – was stolen on Nov.14. The information *did not* include addresses, phone numbers, social security numbers, credit card, debit card, or bank account numbers, but did include some demographic and health information.

The electronic equipment was stolen out of an Omnicell employee's car. A police report was filed, but the equipment has not been recovered. UMHS has determined that the potential patient information exposure occurred because Omnicell's employee stored data on an unsecured electronic device, which is a violation of UMHS' and Omnicell's standard policies and procedures in place to protect private health information. UMHS policy requires that all patient information be stored on an encrypted device – encryption is the strongest and most secure method of protecting data.

Omnicell has also informed the other two affected hospitals of the incident, and those institutions are also preparing to notify their patients.

"Patient privacy is extremely important to us, and we take this matter very seriously," says UMHS Chief Compliance Officer Jeanne Strickland. "UMHS has taken immediate steps to investigate this matter."

An investigation shows that the files on the electronic equipment contained the following demographic information about some patients who were seen between Oct. 24 and Nov.13, 2012: patient name; birth date, UMHS patient number and medical record number. Additionally, one or more of the following clinical information may also have been involved: gender; allergies; admission date and/or discharge date; physician name; patient type (i.e., inpatient, emergency department or outpatient); site and area of the hospital; room number; medication name; and medication dose amount and rate, route, frequency, administration instructions, start time and/or stop time.

As a precautionary measure, affected patients have been advised to monitor their medical insurance statements for any potential evidence of fraudulent transactions using their information. However, UMHS believes the risk of this occurring is low, partly because the data on the file contains multiple fields that

are not readily understood. An analysis of the data would be needed in order to link specific patient names to private health information.

Omnicell is continuing to investigate this incident and is working closely with authorities to locate the stolen equipment and secure all patient information. Omnicell is also taking steps to improve its security program and practices in response to this incident.

Affected UMHS patients are expected to receive letters in the mail notifying them of this incident within the next couple of days. Patients who have concerns or questions may call toll-free (855) 855-4331, Monday through Friday, from 8 a.m. to 5 p.m., and Saturday, from 8 a.m. to 2 p.m.