The MetroHealth System
2500 MetroHealth Drive
Cleveland OH 44109-1998

News Release

FOR IMMEDIATE RELEASE:
May 15, 2015

CONTACT:
Tina Shaerban Arundel
216-778-5370
tarundel@metrohealth.org

Breach Notification from The MetroHealth System

On March 17, 2015, The MetroHealth System discovered malware on three computers in its Cardiac Cath Lab. The malware appears to have infiltrated these computers during the period between July 14 and July 19, 2014. The malware was isolated to those three computers. The data stored on these computers included medical information on 981 patients who had cardiac catheterizations from July 14, 2014 to March 21, 2015.

Upon learning of the malware, MetroHealth immediately undertook a detailed forensic assessment of the malware and its computer networks. The investigation revealed that (1) one of MetroHealth's business associates updated software systems used on these computers during the period that the computers were infected (July 14, 2014 through July 19, 2014), (2) during the update, the antivirus protection for these computers was disabled to facilitate the updates, (3) malware was able to infect these computers as a result of the disabled antivirus protection and (4) this malware was removed on March 18, 2015. In addition, the malware created a "back door" for potential subsequent access to those computers. MetroHealth has no evidence of any subsequent access. The "back door" component of the malware was successfully purged from those computers on March 21, 2015.

In accordance with federal law, MetroHealth is in the process of notifying cardiac catheterization patients whose information was stored on one of these computers during this time.

While unlikely, it is possible that this unauthorized access could lead to a compromise of some patient information. MetroHealth has no indications that the information has been accessed or used by any unauthorized individual. The circumstances surrounding the event and typical uses made of this malware indicate that the computers were hacked in an effort to obtain banking information and credentials used to log into financial accounts. No such information is stored on these computers.

MetroHealth has no evidence that the malware is used to obtain medical information. The information that is stored on these computers is considered to be Protected Health Information ("PHI") and consists of:

> Patient name; date of service; date of birth; height; weight; medications administered during the procedure; medical record number; case number (limited to only to that procedure); and cardiac catheterization raw data such as tracings of EKG and oxygen saturation.

There is no evidence that any of the patients' information has been inappropriately accessed or used. Nevertheless, those patients are being advised to monitor account statements and explanations of benefits for health care services related to their Cath Lab procedure.

MetroHealth is keenly aware of how important PHI is. We sincerely apologize and regret that this situation has occurred. MetroHealth is committed to providing quality care while protecting the privacy of our patients. In light of this incident, we have strengthened our procedures to better protect patient privacy, including:

- Initiated a complex forensics security investigation
- Increased the monitoring of computers for Malware
- Added antivirus update reviews
- Revised our incident response plan
- Revised our Cath Lab software update procedures

We will continue to do everything we can to strengthen our operational protections. Any patient with questions about this should contact Joseph A. Dickinson, Privacy & Information Security Officer, jdickinson@metrohealth.org. 216-778-5776.