Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

September 2011 - Issue 20

What's Inside?

Recover Crashed Hard Drives Only with Authorized UM Vendors

Computer hard drives and other electronic storage media routinely fail, leading to potential data loss or corruption. It's not just personal computers and servers; many medical and laboratory devices may also store data on such devices. It is important to make secure, backup copies of any critical data to guard against such failures. One such measure is to store or copy critical data on a secure, network drive where routine backups are performed by your IT support. Some IT support groups may backup critical desktops, but as a general rule, local hard drives are not routinely backed up. However there may be cases where vitally important data resides on a PC, laptop or lab device and backups were not performed, are incomplete or data cannot be recovered for some other reason. The hard drive/storage device has failed and this vitally important data needs to be recovered if possible. In such cases you may need the services of a data recovery company. These companies use specialized tools to recover data from failed storage media. Yet here too there are risks. Your hard drive could potentially contain identifiable information on patients, research participants, employees or students. It could contain other intellectual property, confidential business plans or other information not for public distribution. The University has contracts with the following companies to provide data recovery services. Such contracts obligate the company to securely handle any confidential information and serve to protect the University should there be a data breach or loss of the University's confidential data at such a vendor. Contact your official IT support group for assistance. The list of vendors authorized to provide such services include:

Computer Based Associates
http://www.netcba.com

DriveSavers
http://www.drivesaversdatarecovery.com

Federal HIPAA Audit Program Details Emerge

The HIPAA compliance audit program mandated by the HITECH act is expected to begin soon, with about 150 on-site audits of covered entities and business associates anticipated by the end of 2012. The Department of Health and Human Services has awarded a $9.2 million contract to the consulting firm KPMG to develop the protocols and conduct the HIPAA audits. "Site visits conducted as part of every audit would include interviews with leadership (e.g., CIO, privacy officer, legal counsel, health information management/medical records director); examination of physical features and operations; consistency of process to policy; and observation of compliance with regulatory requirements."

Every site visit will result in a detailed audit report. The HHS Office for Civil Rights will oversee the audit program.

Privacy & Security News

Tackling Medical Device Security Issues

Best practices for protecting medical devices are sorely lacking. The recently formed Medical Device Innovation, Safety and Security Consortium is attempting to devise risk management best practices for keeping medical devices secure. The security of medical devices is a significant risk management issue because the devices increasingly are linked to networks and exposed to malware, which could impair their functionality and potentially adversely affect patient safety. Many medical devices, such as heart monitors and infusion pumps, are linked to computer networks, and many of those networks are becoming linked to others, "We have a national biomedical device network that remains largely unrecognized," says Dale Nordenberg, M.D., founder of consortium. "Malware and security risks are evolving very fast," Nordenberg notes. As a result, the industry needs to consider whether the security of devices approved by the Food and Drug Administration needs to be regularly revisited, he argues. Nordenberg was one of several speakers addressing medical device security at an information security conference co-sponsored by the Department of Health and Human Services' Office for Civil Rights and the National Institute of Standards and Technology.

(continued on next page)

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.med.miami.edu/hipaa
Phone: 305-243-5000
Fax: 305-243-7487

Genomics Research: Privacy Issues

Personalized medicine research, which relies on genetic information paired with electronic health records, could pave the way for many treatment breakthroughs. For example, diabetics could get the precise therapy they need, based on their genetics, to avoid amputations. The Department of Veterans Affairs has unveiled a national effort to recruit veterans to participate in an ambitious genomics research project. A website for the Million Veteran Program outlines multiple security measures for the effort. For example, DNA samples and records will be labeled with bar codes, and researchers won't have access to veterans' demographic information. The VA has an ambitious goal of signing up 1 million participants, reassuring them that their privacy will be adequately protected. The HITECH Act mandated a federal study on the issue of de-identification of data for research purposes and whether existing HIPAA regulations on the subject need to be modified.

Secret Service Probing Records Theft at Troy Regional

U.S. Secret Service agents say the theft of personal information from patient records at Troy Regional Medical Center (TRMC) is connected to an investigation that reaches across county lines. "Currently our office is investigating a case of identity theft and a part of that investigation involves the compromise of personal identifiers related to the hospital in Troy," said Clayton Slay, the lead Secret Service agent. Troy Regional Medical Center administrators said that personal information from 880 of its former patients was illegally accessed and removed from the hospital's records earlier this year. Teresa Grimes, CEO and administrator at TRMC, said Tuesday authorities were concerned the information obtained from the records could be used to file fraudulent income tax claims. The hospital staff is working this week to notify the patients involved in the incident. "We greatly regret this incident and we are committed to protecting our patients' information and to providing assistance to protect the personal information of the patients affected," Grimes said. "When we learned of the breach, we immediately initiated our own investigation," Grimes said. "We are developing and implementing a corrective action plan to better protect our patients' personal information". The hospital also is requiring immediate, mandatory training to all employees regarding the protection of patient information.

Nurse Accused of Illegally Accessing Thousands of Medical Records

A nurse who worked at Memorial Hospital in Colorado Springs is accused of accessing 2,500 medical records for personal use. Investigators say Lori Neill was accessing these records without a medical, billing, or operational reason. Memorial Hospital said the nurse worked in the Occupational Health Clinic. Investigators said she was unlikely to be using the information for identity theft, but won't comment any more as to why they say she accessed the files. Memorial Chief Executive Officer Dr. Larry McEvoy said they are both saddened and angered by the accusations. "People entrust us with their lives and most intimate details. They turn to us for safety, privacy and respect, and that's a special trust we take seriously," McEvoy said in a statement. Memorial has since formed a task force to increase security, to prevent something like this from happening again. They're also exploring other computer systems that will detect unusual medical record activity more quickly.

Ignored Password Security Policy Leads to School Data Breach

The headmaster of a Hampshire comprehensive school has been forced to apologize after a student hacked into the school's systems and exposed thousands of personal records. The attack, which took place at Bay House School was immediately reported to the Information Commissioner's Office (ICO) and the school must now initiate a public undertaking to better enforce its own security policies. The ICO said the personal details of nearly 20,000 individuals, including some 7,600 pupils, were put at risk during an attack on the school website. The files compromised included some medical information about pupils, as well as information about parents and teachers. According to the ICO, the attack was made easier because a member of staff was using the same password to access both the school's website and data management systems. Having discovered the staff member's password while hacking into the remote-hosted website, the pupil was able to access the school's own administration systems. The school said it had advised staff to avoid the use of duplicate passwords, but did not enforce the policy. The school has agreed to "encrypt and segregate sensitive and confidential information" and re-train staff on security awareness including password policies. The school will also now undergo an annual penetration test.

Related Links

- **Medical Devices:** http://blogs.healthcareinfosecurity.com/posts.php?postID=956
- **Genomics:** http://www.research.va.gov/MVP
- **Records Theft:** http://www.troymessenger.com/2011/07/07/secret-service-probing-records-theft
- **Nurse Accused @ Becker's Hospital Review:** http://goo.gl/G10tp
- **School Data Breach:** http://infosecmedia.org/ignored-password-security-policy-leads-to-school-data-breach

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.med.miami.edu/hipaa
Phone: 305-243-5000
Fax: 305-243-7487