Included in this newsletter is guidance on various HIPAA-related topics that impact your everyday work life. Hopefully, it will help answer some of your questions about how HIPAA relates to your work.

Email Breaches Lead to ‘Wall of Shame’

Several recent large data breaches involving email mishaps serve as a reminder of precautions that healthcare entities must take with protected health information contained in digital communications that are sent or received by their organizations.

Among recent incidents listed on the Department of Health and Human Services' "wall of shame" website of HIPAA breaches affecting 500 or more individuals are two incidents at the North Carolina Dept. of Health and Human Services. Another reported incident, not yet publicly posted on the HHS website, occurred at the University of Cincinnati Health.

In both North Carolina DHHS breaches, which were discovered about a month apart, employees sent unencrypted email messages containing PHI to other local health departments in the state. One incident affected more than 1,600 individuals, the other DHHS breach about 524 people.

In a statement, the North Carolina public health officials say, "DHHS cannot determine for certain that the email was not intercepted during transmission over the Internet, but has no reason to believe any information was compromised. DHHS is reminding staff to encrypt emails containing confidential information prior to sending, and is also exploring technology that will encrypt emails automatically to avoid human error in the future."

PHI exposed in those incidents include names, Medicaid recipient ID numbers, Social Security numbers, dates of birth, addresses, gender, ethnicity, race, insurance information and healthcare provider names.

Meanwhile, the University of Cincinnati Health says its recent breach, affecting a total of 1,064 individuals, involved email messages that were sent to the wrong domains on nine occasions over a period of about a year.

In a statement, UC Health says, "emails containing PHI that were intended to be sent internally within UC Health were inadvertently sent to an incorrect email address at a domain similar to UC Health's authorized domain. The mistake was made when two letters were transposed in the email address domain name."

Common Problems

Some privacy and security experts say HIPAA breaches - large and small - involving email are a persistent problem for many healthcare entities.

"I believe email is a common source of breaches," says Rebecca Herold, partner and co-founder of the consulting firm SIMBUS Security and Privacy Services. "Many people are very nonchalant about making such mistakes," she adds. "In this year alone I've had a lawyer, a privacy officer and an information security officer all accidentally send me email messages they had meant for other 'Rebeccas.'"

Herold says she believes most people erroneously receiving such messages probably don't bother to notify the senders of the errors, and most senders don't check to ensure their intended recipients actually received the message. "Most people assume email delivery is guaranteed, and most don't think about the possibility that they made a mistake and sent a message to the wrong person," she says.

Such errors can potentially translate to massive breaches, especially if there are unencrypted attachments, such as spreadsheets, containing PHI for lists of patients, as was in tools to identify when PHI is within emails going outside of the network to then flag them, the case in both recent North Carolina DHHS email breaches.

"Using data leak prevention tools can be used to stop clear text PHI in emails from being sent to recipients outside of the network, and within the network," Herold says.

When it comes to preventing breaches like the one at the UC Health involving misdirected emails, Herold recommends shutting off the

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit: http://www.purdue.edu/hipaa or contact: Joan Vaughan, HIPAA Privacy Officer, jvaughan@purdue.edu or x61927
The incidence of cyber security breaches within the healthcare industry has been growing over the years. For the fourth consecutive year, the healthcare industry had the most breaches among industry verticals, according to the Symantec 2015 Internet Security Threat Report. Because of the high incidence of breaches along with the rise of mobile device usage, practicing high security of sensitive healthcare data is critical.

Protected Health Information (PHI) is increasingly sought by cyber criminals. According to researchers, PHI is more valuable than credit card information on the dark web (or black market). PHI is being sold among cyber criminals for 10-20 times that of credit card information. According to Reuters, PHI being stolen includes names, dates of birth, insurance information, diagnostic codes, among other information. This information is sold to other criminals to purchase prescriptions, purchase medical equipment, or file fake claims with insurance.

According to the Symantec 2015 Internet Security Threat Report, the high incidence of PHI breaches is largely due to poor computer security practices within hospital settings, vulnerable outdated operating systems and software, and insecure practices with mobile device usage.

**There are multiple safe practices, that should be in place by those who are dealing with PHI.**

1. Create strong passwords. Passwords should be longer than 8 characters, and should include a combination of upper and lower case letters, numbers, and special characters. Names, or other words that can be associated with you, should not be used. Do not write down or store passwords in lists, such as Word, Excel, or Notes. These items may be easily accessed if your computer becomes infected with malware and remote access tools are then used on the compromised computer.

2. Use passwords on phones, cloud storage services, and any systems that are accessing PHI.

3. Update programs as they become available. Patches are continually being released to fix vulnerabilities in software. If these are left out of date, then the computer is more likely to be compromised in a cyber attack.

4. Use multifactor authentication when possible. Often, companies will have this feature set up so when attempting to access a system you first enter your password, then a text, call, or email is sent to you requiring you to accept or decline in order to access that system. This way, if someone is attempting to access the system without your knowledge you can decline access to prevent the unauthorized access.

5. Keep your mobile devices with you at all times or store them in a secure location. Enable password protection and auto lockout. Disable wireless access, including Bluetooth, when not in use. Encrypt your mobile device so, if stolen, data will not be accessible.

6. Review application permissions before installing mobile apps. Many applications often share personal information.

---

**Malicious Incidents**

Of the 1,390 major HIPAA breaches listed on the wall of shame as of Nov. 19, 116 involve email. Some, like the recent incidents at the North Carolina Department of Health and Human Services, which affected nearly 228,500 enrollees of the state’s Medicaid program.

In that breach, a former state employee in November 2014 was sentenced to three years of probation, plus community service, after pleading guilty to four counts of willful examination of private records by a public employee and one count of criminal conspiracy.

Besides email incidents involving intentional and accidental unauthorized disclosures of PHI, the HHS wall of shame is also splattered with a variety of major breaches involving email and hackers.

Among the largest email breaches involving malicious, unauthorized access or disclosure was a 2012 incident at the South Carolina Department of Health and Human Services, which affected nearly 228,500 enrollees of the state’s Medicaid program.

In that breach, a former state employee in November 2014 was sentenced to three years of probation, plus community service, after pleading guilty to four counts of willful examination of private records by a public employee and one count of criminal conspiracy.

Besides email incidents involving intentional and accidental unauthorized disclosures of PHI, the HHS wall of shame is also splattered with a variety of major breaches involving email and hackers.

Among the largest email breaches involving malicious, unauthorized access or disclosure was a 2012 incident at the South Carolina Department of Health and Human Services, which affected nearly 228,500 enrollees of the state’s Medicaid program.

In that breach, a former state employee in November 2014 was sentenced to three years of probation, plus community service, after pleading guilty to four counts of willful examination of private records by a public employee and one count of criminal conspiracy.

Besides email incidents involving intentional and accidental unauthorized disclosures of PHI, the HHS wall of shame is also splattered with a variety of major breaches involving email and hackers.

---

**Steps to Take**

Experts recommend a number of measures that organizations should take to reduce the risk of breaches involving email.

For incidents involving unauthorized disclosure, “most email filters have at least a lexicon - as simple as a word list or weighted word list - to sense when PHI and other sensitive data types are being sent, then auto-route for encrypted delivery - or data in motion,” Dill says. “Making users aware of other key words that can be an encryption trigger like ‘confidential’ or setting the sensitivity flag before sending - can be coded to auto-route for secure delivery,” he adds.

Still, “data loss prevention tools will likely do the best job to monitor, alert, quarantine for review, forward and encrypt, and/or block based on job role - to enforce corporate appropriate use rules,” Dill says.

“Emerging market place tools provide encryption with lifecycle management tools - where the file has to ‘check in’ before use,” he notes. “When the sending organization has the encryption key, they can always control what can be done with the file, and by whom - deleting the key when they choose, rendering the file a useless blob.”

Herold notes that to reduce the risk of phishing related breaches, “training is essential.” she says. The training should also provide examples and case studies of phishing attempts that succeeded, and the damage they caused, she notes.

Full article at:  [http://www.healthcareinfosecurity.com/email-breaches-lead-to-wall-shame-a-8695](http://www.healthcareinfosecurity.com/email-breaches-lead-to-wall-shame-a-8695)