Risk Reporter
for Senior Living Communities
A quarterly publication by Church Mutual Insurance Company
Summer 2014 | Vol. 15 issue 2

HIPAA changes mean data security more critical than ever

Imagine this: Your administrator takes her work laptop home for the weekend. On the way she stops for groceries, her car is broken into and the laptop is stolen.

Minor hassle or major problem?

In the past, lost data had to meet a risk of harm standard to be considered a breach. Changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mean covered entities must now assume any lost, stolen or otherwise compromised personal health information (PHI) is a breach unless the entity can prove otherwise.[1] And because that's nearly impossible, data loss is now a much bigger issue.

"There were two recent million-dollar-plus fines that were based on the number of people whose PHI *could* have been compromised," said Matthew J. Murer, chair of national healthcare practice at Polsinelli, PC in Chicago.

"Internal fraud, social engineering, lost and stolen equipment, misguided emails and accidental website postings are major contributors to data loss," said Tom Widman, president and CEO of Identity Fraud Inc., a company that provides identity fraud solutions and cyber insurance for organizations.

Which isn't to say third-party data theft isn't also a problem. "Criminal attacks on healthcare systems have risen 100 percent since 2010," said Michelle Manu, JD, director of risk and legal affairs for Silverado Senior Living in Irvine, Cal.

Is your facility subject to HIPAA?

The answer is likely *yes*. "If you engage in covered transactions and bill electronically, you're a 'covered entity,'" Murer said.

You also could be subject to HIPAA as a "business associate," defined by the U.S. Department of Health and Human Services (HHS) as conducting "business with a covered entity that involves the use or disclosure of individually identifiable health information."

"Your facility is unlikely to be a business associate, but your data processor, lawyer or accountant could be yours," Murer said. "Have the appropriate agreements in place to protect yourself."

"HIPAA includes both a data privacy rule and a data security rule," Widman said. "Compliance requires technical controls and steps to

(See Data security, Page 2)

[1] http://www.alfa.org/News/3520/New-HIPAA-Rules-Are-Assisted-Living-Game-Changer

Inside

cont.

(Data security)

limit who can access medical records and control how information is shared. There's also an employee awareness-training component, and security training is mandatory if handling medical records."

Steps to improve data security

Educate employees

At Silverado, all employees received HIPAA and Health Information Technology for Economic and Clinic Health Act (HITECH) training and took a proficiency exam. Associate disciplinary guidelines related to PHI are now in place.

Build breach protection into your policies

Silverado employees are not allowed to use flash/thumb drives and there's no texting or emailing of PHI to outside parties. Documents are automatically saved to servers and web servers with the necessary firewalls. The company's privacy policy addresses when PHI should be disclosed, produced or requested and how it will be transported.

Instruct employees to lock up paper data, avoid leaving resident records out, log out of unattended computers, secure hardware and shred all vulnerable paper data.

Employees should know never to view, open or copy an email attachment unless they know who sent it *and* expect the file or link. Require regular password updates.

Install virus software and firewalls

"Skilled hackers can get into any system, but basic defenses can make you less appealing," Widman said.

Security expert Symantec Corporation recommends:

- **Antivirus and behavioral malware prevention.** Stops malware from disrupting your computer's operation.
- **Bi-directional firewalls.** Filter incoming/outgoing traffic; protect vulnerable applications/services.
- **Browser protection.** Protects you from web-based attacks.
- **Reputation-based tools.** Check reputation/trust of a file or website before downloading.[2]

Update, update, update

Old versions of your software, web browser and operating system can have security problems. Set your system to automatically check for updates; only use those that come directly from vendors. Take care of updates pronto. Still using Windows XP? Replace it. As of April 8, 2014, updates were no longer provided.[3]

Limit email attachments

Symantec suggests configuring mail servers to block or remove any email that includes a file attachment-type used to spread viruses, such as .BVS, .BAT, .EXE, .PIF and .SCR.

[2] http://www.symantec.com/connect/blogs/symantec-2014-internet-security-threat-report
[3] http://windows.microsoft.com/en-us/windows/end-support-help

Wipe the data slate

"You must be able to remotely wipe data from all hardware," Murer said. "Follow a policy of removing all data before you trade in or salvage a copier or computer and maintain records on where that hardware went."

Consider data encryption

While not mandated by HIPAA, your facility should investigate if this is worthwhile.

Stay informed

"Be proactive," Manu said. "Stay connected with the Health Care Compliance Association and research recent OCR (Office of Civil Rights) infractions, penalties and correction instructions."

Be wary of mobile/personal devices

"Mobile devices offer great efficiencies, but they also introduce a whole new frontier of exposure," Widman said. "Your staff should only access your business network if their devices have been scanned for vulnerabilities and approved for use."

Develop effective breach response

Develop an incident response plan now that dictates the steps you'll take if a breach occurs and identifies your response team and their roles. Address both HIPAA and state-specific notification rules.

At Silverado, the privacy officer takes the following steps if notified of a potential breach: alerts all interested internal parties, conducts a risk assessment to determine if breach occurred, records breach in a disclosure log, if reportable — and depending on severity — notifies the HHS Secretary (self-report), media (press release) and all individuals impacted by a reportable breach (letter and credit monitoring), as per HITECH.

"Your staff must work together to get to the bottom of a problem and address it," Manu said. "It's not about finger pointing."

Consider cyber liability insurance

Addressing a data breach can be time consuming and very expensive. Church Mutual is working with CMIC Specialty Services and Identity Fraud Inc. to offer a cyber liability insurance and data breach services program to our customers. Please contact your Church Mutual representative or agent for more information.

Resources:

- Complimentary risk assessment through Identity Fraud Inc.: http://hipaasafeguard.com/RiskAssessment.aspx.
- HIPAA's covered entity criteria: https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/CoveredEntitycharts.pdf.
- An overview of the impact of recent HIPAA changes: http://www.alfa.org/News/3179/Changes-to-HIPAA%3A-How-New-Privacy-Rules-Will-Affect-Your-Business.

Managing Your Risks

Ladder Inspection Checklist and safety posters

Ladder-related slip-and-fall accidents are a significant cause of claims to Church Mutual. During 2009-2013, employees and even some residents and guests were involved in 870 ladder accidents costing more than $13.8 million. Injuries to maintenance workers were responsible for the biggest share of the workers' compensation claims and associated dollar losses.

Trimming trees, painting, repairing roofs and changing light bulbs are just a few of the many tasks that often require using a ladder. Because ladders are used frequently, it's easy for employees to overlook potential hazards when using them.

To help address the proper use of ladders and related safety concerns, Church Mutual developed a new ***Ladder Inspection Checklist*** that outlines five key steps for using ladders safely:

- Choosing the right ladder
- Inspecting the ladder
- Correct set up
- Climbing and descending
- Using safe work practices

The brochure includes four tear-out copies of the checklist. There also are four *Danger — Damaged Do Not Use* tags that can be attached to a defective ladder to warn others about its condition and to indicate it is "out of service."

Six new safety posters were added to the risk control resources available to Church Mutual customers. These posters provide helpful tips for employees and others about preventing back injuries, kitchen accidents, strains and sprains and slips and falls on walking surfaces and from ladders. Also, information on assisting residents and making ergonomic adjustments to computer workstations is covered in two of the posters. To view, download or print copies of these and other safety resources, please visit our website at www.churchmutual.com.

Edward A. Steele
Risk Control Manager

SeasonalSpotlight

Formal building and grounds inspections a must

Facility best practices already dictate that your staff is conducting informal facility inspections as they go through their daily routines. Do you still need to conduct more formal checks? According to Ed Steele, Church Mutual's risk control manager, the answer is a definite "yes."

"The daily checks are critical to address urgent issues and help you catch small problems before they turn into big ones," Steele said, "but regularly scheduled formal checks are equally important."

Aim for monthly. "This is the ideal — conduct them quarterly at a minimum," Steele recommended.

Take a team approach. The administrator, the person in charge of buildings and grounds and the safety committee — if you have one — should all be involved. "We all have our blind spots," Steele said. "It's valuable to see things from different perspectives."

Use a checklist. This ensures thoroughness and consistency. Factor in the main exposure concerns based on your resident categories (age, mental and physical acuity), facility (age, type and layout), location and security challenges. Ask for input from all departments when developing your checklist. This helps ensure you're not missing problem areas that only someone who's intimately familiar with an area or task might notice.

"Many of our customers have multiple facilities," Steele said. "They work at the corporate level to develop a standardized list, and then each facility adapts it to its needs."

Don't have a checklist? Church Mutual's self-inspection recommendations are a good starting point.

Take pictures. "These help you to accurately capture facility concerns and can be a valuable tool if you need to convince upper management that a repair or update is necessary," Steele said.

Consider adding transportation vehicles to your checklist. "Some facilities break this category out separately, but I typically recommend including facility vehicles in this inspection," Steele said.

Document, prioritize and take action. Your inspection only has value if it drives change. Develop a list of problem areas, determine what steps you'll need to correct them and rank them. "Some fixes will be easy and inexpensive while others might require a budget line item," Steele said. "And, of course, you must prioritize problems that could put residents, staff or visitors at risk."

Recognize that money isn't the answer to every issue. "Sometimes you need to change behavior or attitude," Steele said. "Work with administration or HR to determine changes in training that will address your problem areas."

Q|A

A Perspective

When an employee is hurt on the job, filing an insurance claim might seem low on your list of priorities. But there are a number of reasons why it's critical to report the injury to your insurance company within one business day. Risk Reporter recently spoke with Jennifer Wolf Horejsh, executive director of the International Association of Industrial Accident Boards and Commissions (IAIABC), to learn more.

Founded over a century ago, the IAIABC was created to improve the efficiency and effectiveness of workers' compensation systems around the world. Additional information can be found at iaiabc.org and OSHA has a useful worksheet on workers' compensation at https://www.osha.gov/Publications/safety-health-management-systems.pdf.

Risk Reporter: **Why do injuries go unreported?**

Jennifer Wolf Horejsh: An employee might think the injury is no big deal, fear being reprimanded or worry co-workers will think differently of them. A company might believe reporting an injury will cause its insurance rates to go up. One thing that's become clear over the history of IAIABC is that it's best practice to report every injury.

Risk Reporter: **IAIABC research shows costs start to go up if reporting is delayed even a week. Why?**

Jennifer Wolf Horejsh: A delay can exacerbate a medical problem and complicate treatment. It can also hinder the accident investigation process, which could increase the chance of a workers' comp claim denial and lead you to incur costs in the dispute resolution process. If the injury was the result of a dangerous situation, more people might be hurt because the problem wasn't resolved. Delayed reporting can also slow return to work. Research shows the longer an employee is out of work, the less likely he or she is to return to work. Delaying return to work will drive up indemnity costs, and delaying appropriate medical treatment could compromise employee recovery. Delays could also lead to fines or penalties from your state.

Risk Reporter: **What are some things to be aware of during the return to work process?**

Jennifer Wolf Horejsh: Work with the claims adjuster, the employee and his or her medical provider to understand a reasonable timeline for returning and if accommodations will be necessary to avoid reinjury. Research supports the value of returning to work, but it must be done appropriately.

Risk Reporter: **Please address the importance of a safety culture.**

Jennifer Wolf Horejsh: This must be integral to your organization. Work to ensure employees understand safety rules and best practices — discuss them frequently and regularly. An accident is a good time to revisit your safety protocols. Talk about the accident in a neutral environment, and use it as a learning lesson. Determine if protocols are appropriate. Do you provide the staffing and support needed to follow them? Employees must know they can't be fired for filing a workers' comp claim — it's a no-fault system and their injuries will be covered even if the accident was their doing.

Church Mutual Insurance Company | www.churchmutual.com
3000 Schuster Lane | P.O. Box 357 | Merrill, WI 54452-0357

Interim Editor: Patrick M. Moreland | (800) 554-2642 Ext. 4833 | pmoreland@churchmutual.com
Risk Control Advisor: Edward A. Steele, CSP, ARM | (800) 554-2642 Ext. 4403 | esteele@churchmutual.com
Writer: Vicky Franchino | **Layout:** Dan Kaminski

Church Mutual® INSURANCE COMPANY
Listening. Learning. Leading.®