PULSE

March 2012 • Vol. 28 No. 3

www.acainternational.org

PUBLISHED FOR HEALTH CARE PROVIDERS BY
ACA INTERNATIONAL'S HEALTH CARE SECTION

# Security Breach Implications

**By Katie Hebeisen, Communications Specialist**

The Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), set forth requirements for covered entities and business associates to provide notice to affected individuals, media and the Department of Health and Human Services (HHS) following a breach of unsecured protected health information (PHI). Most states have also enacted laws requiring similar forms of notification following a security breach.

While breach notifications strengthen privacy and data security initiatives, reporting a security breach can have drastic effects on a business, including monetary loss and harm to a company's reputation.

At ACA's 2011 Fall Forum session, HIPAA/HITECH Updates, Leslie Bender, president of Bender & Radcliffe, P.A. in Timonium, Md., discussed security breach implications and why businesses need to fully understand their legal duties following a data security or privacy incident.

"Not every security incident will trigger a breach notification," Bender said. "And there are good business reasons why you do not want to provide a notice in response to all security incidents."

## Security Incident vs. Security Breach

HIPAA and HITECH draw a distinction between a security incident and a security breach. While all security breaches are security incidents, not all security incidents turn out to be security breaches.

The law defines a security incident as "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system."

Common types of security incidents include impermissible uses and disclosures of PHI and lack of safeguards of PHI.

A breach is defined under HITECH as "the acquisition, access, use or disclosure of protected health information in a manner not permitted [under HIPAA's Privacy Rule], which compromises the security or privacy of the protected health information."

Importantly, a breach must "compromise the security or privacy of the protected health care information," which means it poses a significant risk of financial, reputational or other harm to an individual.

"There have been reported instances where, for reasons unrelated to HIPAA, organizations are insinuating that any violation of HIPAA's Privacy Rule, even if inadvertent, equals a breach and should be reported to HHS," Bender said. "That's simply not true."

Some workers in health systems are not aware of what a breach actually means. A business must communicate with its employees what constitutes a security breach and what does not.

Bender provided three examples of situations that would not be considered a security breach:

1. An employee in your office has permission to go into your database accidentally looks up the wrong information.
   "If someone calls a representative and says 'My name is Leslie Bender,' it's possible you would have more than one Leslie Bender in your database," Bender said. "So when the representative is scrolling through to find the right Leslie Bender, it's possible that person could look at something they shouldn't have looked at."
2. An employee accidentally discloses information to someone from another company who may have a business purpose to access the information in some cases, but this time it was done in error.
   "In this instance, you're trying to send information to an insurance company, but it accidentally gets sent to the wrong business," Bender said. "But the person who gets it is probably not going to use or disclose it in a manner not permitted by HIPAA's Privacy Rule since they are already bound to comply with it."
3. An employee accidentally discloses information to someone outside the organization who does not have a business purpose to access the information, but who upon receipt of it agrees not to disclose the information any further (and you are confident this is true).
   "In this instance, the person it was

*continued on page 2*

PULSE
March 2012

# Growth in U.S. Health Spending Remained Slow in 2010

U.S. health care spending experienced historically low rates of growth in 2009 and 2010, according to the annual National Health Expenditures report released by the Centers for Medicare and Medicaid Services.

Data shows the low rate of growth reflects lower utilization in health care than in previous years. U.S. health care spending grew only 3.9 percent in 2010, reaching $2.6 trillion or $8,402 per person, just 0.1 percent faster than in 2009.

As health spending growth remained low in 2010, growth in the U.S. economy, as reflected in gross domestic product, rebounded. As such, the health spending share of the overall economy was unchanged at 17.9 percent in 2010. In the past, this share has increased, rising over time from 5.2 percent in 1960.

# Research Suggests Hospital Mergers Offer Few Benefits

Despite the trend of hospital mergers and acquisitions, new research from the Centre for Market and Public Organisation (CMPO) indicates mergers are not the most effective way to handle hospitals that are performing poorly in quality or costs.

The research found poor financial performance typically continued following a merger, with hospitals that merged making larger deficits post-merger than pre-merger. Also, the length of time people had to wait for elective treatment increased after the mergers. Further, the report showed no increase in activity per staff member employed in merged hospitals, and few indications of improvements in clinical quality.

Although the rationale varied for consolidation from place to place, the main reasons for mergers were reducing excess capacity, returning hospitals to financial health and producing better outcomes for patients. According to the CMPO, "Mergers offer much before the event, but often fail to deliver on their promises."

## Security Breach Implications

*continued from page 1*

sent to calls up and says 'What's going on? I received someone else's information in the mail. Do you people have a privacy problem?'" Bender said. "At which we would reply, 'We regret inadvertently sending the information to you. Please be assured privacy is important to us. We would ask you to shred the information or return it to us.' Once you have received the recipient's assurance the information will not be used further, the inadvertent disclosure does not constitute a breach."

### Business Implications

Breach notifications can have severe long-term effects on a company, including reputational damage and monetary loss.

HHS is required to maintain a listing of all breaches for which notice has been received. This listing of breach notices is published publicly and readily searchable. Many states also publish breach notices.

"Every time you give a breach notice to a consumer in Maryland, you have to send it to the Attorney General's office and the Attorney General publishes it," Bender said. "So when collection vendors are competing in an RFP, the prospective clients can go in and see if the vendors have committed a data security breach."

Reporting security breaches can be very costly for a business. The cost of security breaches tend to be higher in health care situations because consumers are even more displeased if their most trusted information is used in a way they do not expect.

"Data security breach incidents in the United States are on the rise," Bender said. "The cost is over $200 per compromised record, most of which relates to you protecting your business reputation."

Reporting security breaches becomes a very serious issue because most of the costs relate to preventing customer turnover and preserving business relationships.

According to Bender, surveys document that consumers often do not suffer much actual loss from a security breach. "A company can mitigate the harm to consumers," Bender said. "But it is very difficult to manage the loss to a business."

Because of the overall costs of reporting a breach and the harm it can do to a company's reputation, it is important to only provide notice of a security breach when it is absolutely necessary.

"Providing breach notices is most likely going to hurt your business," Bender said. "This doesn't mean don't do it, it means be careful when you do it."

# ICD-10 Adoption Brings Changes to Medical Coding Practices

**By Kristie Danielson, Paralegal**

Since the 1900's, the U.S. health care system has followed a standardized disease classification system: the World Health Organization's International Statistical Classification of Diseases and Related Health Problems (ICD) code. Like many developed nations, the U.S. uses ICD to track vital health statistics, such as morbidity and mortality. The U.S. also uses ICD to classify claims for health insurance claim reimbursement.

Currently, the U.S. is the only country in the industrialized world that still uses ICD-9. Because the U.S. is still using the old coding system, U.S. data cannot be compared with other nations who are using ICD-10.

In order to remain up-to-date with current medical procedures and technology, ICD has undergone periodic changes since its inception. In 2009, the Department of Health and Human Services (HHS) issued Final Rule CMS-0013-F, requiring U.S. health care providers to transition from the current ICD-9 system to ICD-10 by Oct. 1, 2013. The transition will impose major changes for health care coders, clinicians and billing managers. Health care providers need to be aware of the impact ICD-10 changes will have on their organization.

## Impact of ICD-10

One benefit of ICD-10 is that the change will provide more detail and specificity, allowing providers to improve payment accuracy and claim adjudication. Additionally, more specific data about diagnoses and procedures may help providers improve their quality of care, utilization management and contract negotiation.

The transition to ICD-10, however, will be costly for providers. A 2003 cost analysis found providers could end up paying up to $8.2 billion for system implementation and up to $1.4 billion for training.[1]

Updates to existing software and system interfaces will have to be implemented, affecting processes of the revenue cycle. Current and new employees will have to be trained on how to properly code diseases and insurance claims. Failure to code claims properly could result in claims being denied, negatively impacting the provider's revenue. Without proper training, productivity could also suffer during the initial implementation months, as individuals may expend extra time ensuring claims are coded properly.

## Implementation Progress

According to a study conducted by the American Health Information Management Association (AHIMA) in August 2011, the number of organizations behind schedule for ICD-10 implementation is rapidly shrinking. According to the AHIMA study, 85 percent of respondent organizations indicated they have started working on ICD-10 planning and implementation. This is up from 62 percent a year ago. Many providers have cited a lack of proper resources as one of the largest barriers facing implementation.

While many organizations have started creating budgets and assessing training needs in preparation for ICD-10 implementation, only half of health care organizations have started making changes.

## Provider Considerations

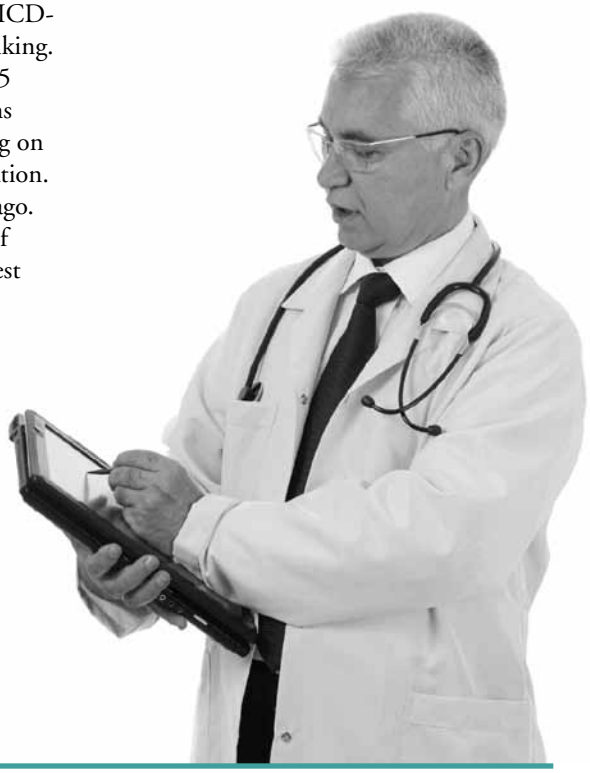
In order to achieve ICD-10 compliance by Oct. 1, 2013, providers need to proactively start ICD-10 preparation. When developing an ICD-10 implementation strategy providers should consider:

- Establishing an implementation planning team;
- Establishing an implementation planning budget;
- Determining how training is going to be conducted (e.g., internally, via Internet testing or at home reading, etc.); and
- Conducting an impact analysis.

Providers that have not prepared an implementation plan could face major billing headaches and loss of compensation due to claim rejections. As the deadline for ICD-10 compliance approaches, providers should be sure to set their processes in motion.

---

[1]Nolan R.E., *Replacing ICD-9-CM with ICD-10-CM and ICD-10-PCS: Challenges, Estimated Costs and Potential Benefits*, Oct. 2003.

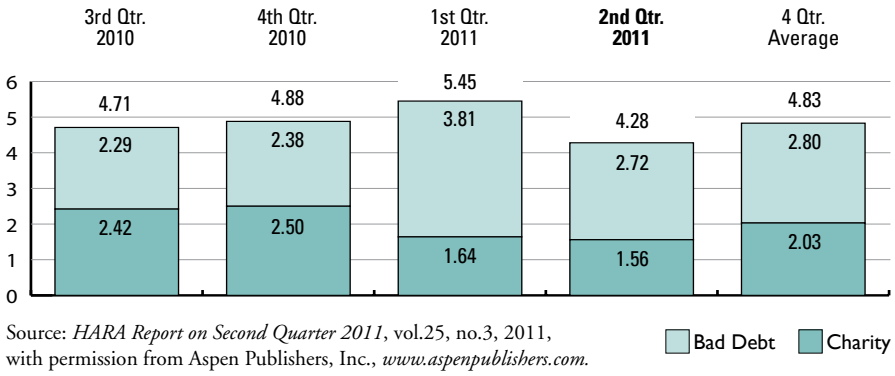


PULSE
March 2012

# DATA WATCH

## Uncollectibles as a Percentage of Revenue

In the second quarter of 2011, write-offs were reduced to 4.28 percent of total gross revenue offsetting a first quarter spike in uncollectible charity and bad debt write-offs. This is more than a full percentage point improvement from the 5.45 percent in gross revenue written off in the prior quarter.




Source: *HARA Report on Second Quarter 2011*, vol.25, no.3, 2011, with permission from Aspen Publishers, Inc., *www.aspenpublishers.com.*

**PULSE** is a monthly bulletin that contains information important to health care credit and collection personnel. Readers are invited to send comments and contributions to:

**Kim Rath, editor**
**Katie Hebeisen, associate editor**

**ACA International**
**P.O. Box 390106**
**Minneapolis, MN 55439-0106**

*Note: Requests for reprints or additional information on material herein must be made through the Health Care Section participant who sponsored your receipt of this publication.*

Do we have your correct name, title, address and zip code? Please advise your sponsor of any corrections.



ACA™ INTERNATIONAL
The Association of Credit and Collection Professionals