

Volume 15, Number 3
Summer 2009



A risk management tool for the healthcare industry

Perspectives

A close-up photograph of a computer keyboard, with a semi-transparent blue circular overlay at the top. The keys are dark, and the 'Enter' key is clearly visible in the foreground.

In this issue:
Managing the risks of data breaches

Table of contents

Managing the risks of data breaches 1

How to make a large scale disclosure of a medical error 7

Managing the risks of data breaches

The use of electronic medical records (EMR) and other digital health information in hospitals continues to grow. At this time, about 20 to 25 percent of hospitals have implemented, or partially implemented, electronic health record systems. This number is expected to rise as the federal government subsidizes the adoption of IT through the American Recovery and Reinvestment Act of 2009 (ARRA). But along with the new funding comes significant new regulations relating to information security. While the adoption of EMR should provide many benefits to the healthcare industry, it also carries risks.

New federal regulations addressing breach of privacy and identify theft will require hospitals to identify and manage these issues. In addition, healthcare organizations need to guard against civil action by individuals whose identity or confidentiality has been compromised. Hospitals also need to determine whether they have the right insurance coverage to help handle the costs of managing these exposures.

Data security: Not so secure

While most businesses – and healthcare institutions are no exception – believe their systems are secure, they are often mistaken. It can be a costly mistake. Over the past two years alone in the U.S., it has been reported that nearly 250 million records have been lost or stolen. The cost to an organization of a breach of a single healthcare record was nearly \$300 in 2008. While a few hundred dollars may not seem like a large sum, when multiplied by hundreds or thousands of records breached in a single event, the cost can become enormous.

In a study in 2008, the Ponemon Institute found the total cost for an entity coping with the consequences of a data breach rose to \$6.6 million per breach, up from \$6.3 million in 2007, with liability and breach notification contributing considerably in the numbers.

Forty-six states, the District of Columbia and numerous foreign jurisdictions mandate notification of every individual whose data may have been affected by a breach. This, however, is just the tip of the iceberg for hospitals. Changes in the regulatory environment now mandate public disclosure of data breaches, thereby bringing in closer media and public scrutiny. The cost to an institution's reputation may be incalculable and the loss of public trust for a healthcare facility may be devastating.

New regulations, new exposures

Beginning February 17, 2010 new HIPAA amendments will be enacted via The Health Information Technology for Economic and Clinical Health (HITECH) provisions of ARRA. These rules will mandate significant new privacy provisions

Checklist

While this is not an exhaustive list, some of the important steps every organization should take to prepare for the new privacy environment include the following:

1. Review your facility's Privacy and Security Policies and Procedures to ensure ARRA provisions are incorporated and implemented as they become effective. Remember, these will change over time.
2. Review your facility's existing Privacy Notification to determine whether any revisions are needed. Be certain to have a notification procedure in place, with clear assignments of responsibility.
3. Review and revise your agreements with business associates to make certain they acknowledge their new obligations under ARRA.
4. Provide training to employees with access to PHI regarding ARRA's amendments to HIPAA.
5. Conduct self-audits to ensure your practices comply with HIPAA and ARRA's requirements.
6. Continually review the changing regulatory landscape: HITECH regulations will evolve over time so make certain your compliance keeps pace.

and controls associated with Personal Medical Information/Electronic Medical Records. The proliferation of EMR is strongly promoted by ARRA, while HITECH strengthens the much softer HIPAA regulations currently in place. This combination creates a situation in which non-compliant healthcare organizations are at greater risk for mandatory patient notifications, fines, penalties and lawsuits.

There are also provisions that will more directly affect hospitals and other covered entities. For example:

When a covered entity discovers a breach of unsecured, protected health information, it will be required to notify everyone whose information 'has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.' (Sec. 13402 a)

The legislation defines a breach as:

...the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

The Act defines “unsecured” information as information that is not secured through the use of a technology or methodology as specified by the Secretary of the Department of Health and Human Services (HHS). This could pose a significant risk for hospitals that have not yet brought their systems security up to HHS standards.

What to expect when a breach occurs

While there may be exceptions, such as for unintentional or inadvertent access or disclosure and for ongoing law enforcement investigations,

the regulations define the procedure to be followed in the event of a breach, including:

- **Notification of each individual affected** — or reasonably believed to be affected — must be made within 60 days of discovery by mail, e-mail (if specified as the preference of the individual) or by telephone if imminent misuse is expected.
- **Notification must include** a brief description of the breach, including dates; the types of unsecured information involved; the steps the individuals affected should take to help prevent harm; the steps your organization has taken to investigate, mitigate damage and prevent future breaches; as well as contact information for the organization.
- **Media notification:** In certain circumstances the organization may be required to post a prominent notice on its web site or in local media. If more than 500 individuals are believed to be affected, the organization is required to provide notice to prominent media in the vicinity.

There are additional provisions on how the healthcare organization must report to HHS, which will track data breaches for annual reports to Congress.

ARRA also authorizes increased civil monetary penalties for HIPAA violations, with fines varying depending on whether the organization knew of the breach, whether it was due to reasonable cause or whether it resulted from willful neglect. The levels of fines are tiered by severity, however, the fines can be substantial even in the lowest tier:

- **Tier 1:** If person is not aware of the violation (and would not have known with reasonable diligence), the minimum penalty is \$100 per violation, to a maximum of \$25,000 for the calendar year.
- **Tier 2:** If violation is due to “reasonable cause” but not willful neglect, the minimum penalty is \$1,000 per violation, to a maximum of \$100,000 for the calendar year.
- **Tier 3:** If violation is due to willful neglect and is corrected within 30 days, the minimum penalty is \$10,000 per violation, to a maximum of \$250,000 for the calendar year.
- **Tier 4:** If violation is due to willful neglect and is not corrected within 30 days, the minimum penalty is \$50,000 per violation, to a maximum of \$1.5 million for the calendar year.

HHS audits may also be performed on any violations and are mandated for Tier 3 and 4 violations.

With violations, mandatory reporting and fines all contingent on the HHS definition of “unsecured” protected health information (PHI), it is critically important for healthcare organizations to bring their systems and data protection up to the standard HHS uses or risk substantial costs, both financial and reputational. By definition, “unsecured PHI” is information not protected through use of a technology or methodology HHS has identified as rendering the information secure, i.e., encryption of electronic data or destruction of electronic and/or paper data. While HHS hasn’t



Reported breaches by year

Year	Records lost/ stolen	Records per second	Incidents reported	Incidents per week	States with notification laws
2002	4,960	0.00	3	0.06	0
2003	6,405,000	0.20	11	.21	1
2004	31,895,900	1.01	21	.25	1
2005	55,986,942	1.77	138	2.65	11
2006	49,679,260	1.57	346	6.65	30
2007	162,563,703	5.15	324	6.23	39
2008	84,365,024	2.67	642	12.35	44

Source: <http://etiolated.org/statistics>

1 <http://blogs.consumerreports.org/health/2009/03/electronic-health-records-usage-nowhere-to-go-but-up.html>
 2 <http://etiolated.org/statistics>
 3 Ponemon Institute 2008 Benchmark Study, February 2009

exhaustively identified the technologies and methodologies that secure information, utilizing the two means defined is a minimum level of protection every organization should implement.

Preparation is key

While no organization can anticipate every possible data breach, it is important to understand the issue not simply as a technology concern, but as a financial and reputation risk. As the potential for a breach continues to escalate, hospitals are well advised to review their current insurance coverage to make certain they have adequate protection should a breach occur.

Issues to consider are whether your current plan helps you protect your organization for the financial impact of direct losses (such as digital assets or monies demanded in cyber extortion schemes) and for the litigation that could potentially follow a breach. Consider not only the fines and penalties that may result, but the cost to limit reputational damage, and, of course, the ever-present concern of litigation.

Systems, training and adherence to standards are critical to managing this risk: closing the gaps in your insurance protection is another component of preparation. •

Zurich Security and Privacy Protection

Delivering a broad range of coverages to the healthcare industry

Zurich Security and Privacy Protection policy provides a broad range of critical third-party and first-party insurance coverage, which include:

- Security & Privacy Liability Coverage
- Privacy Breach Cost Coverage
- Business Income and Dependent Business Income Loss Coverage
- Digital Asset Replacement Expense Coverage
- Cyber Extortion Threat and Reward Payments Coverage
- Internet Media Liability Coverage

Our state-of-the-art coverage is combined with the following loss control and prevention services:

- NetDiligence's eRisk Hub – an on-line tool that provides up-to-date information and solutions on cyber risks for customers
- Digital forensic and e-discovery services offered by Deloitte
- National ID Recovery provides pre- and post-breach services
- Identity Theft 911's security breach response.

For more information, including a self-assessment tool, sample policy forms and application visit our website at zurichna.com under Security & Privacy product, or contact Leo Carroll by phone at 212-553-5336 or email at leo.carroll@zurichna.com.

Additional sources

http://www.eriskhub.com/8_ARRA_standards.php

<http://www.ama-assn.org/ama1/pub/upload/mm/399/arra-privacy-provisions.pdf>

http://www.morganlewis.com/pubs/EB_ARRAamendmentsToHIPAA_Webcast_29apr09.pdf

The information in this article was compiled from sources believed to be reliable for informational purposes only. All sample procedures herein should serve as a guideline that you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this article and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

© 2009 Zurich Services Corporation. All rights reserved.



Missed an issue?

To review past issues of Perspectives or other risk management tip visit www.zurichna.com/healthcare.





How to make a large scale disclosure of a medical error

Zurich HelpPoint: A real story for healthcare professionals

In 2001, the Joint Commission implemented a new requirement that hospitals disclose unexpected outcomes to patients. Healthcare professionals and organizations have developed procedures to address this issue, and have become more comfortable doing so over the past eight years. But a different problem is now facing some healthcare organizations – how to disclose a potential adverse event to a large number of patients. Two recent events illustrate this problem.

- In February, 2008 Nevada public health officials announced that nurses at a Las Vegas endoscopy clinic had re-used syringes and multi-use vials, exposing patients to hepatitis C. More than 40,000 patients had to be tested for the disease, and it is thought that more than 100 have contracted hepatitis C. Several lawsuits are pending.
- In July, 2009 at least 1800 patients were tested for Hepatitis C after it was revealed that a surgical technician had diverted fentanyl. She took fentanyl syringes, injected herself, re-filled the syringes with saline, and used them on patients. The technician had Hepatitis C. At the time of this writing, it is not yet known whether any of the exposed patients have contracted hepatitis C from the surgical technician.

These situations have alerted other practitioners to this type of exposure. A physician at a health clinic, upon reading of these incidents, realized that the clinic may also have exposed patients to blood borne diseases. When performing bone-marrow biopsies, the physicians would draw up lidocaine from a multi-use vial to inject a local anesthetic. If more lidocaine was needed, the

physician would change the needle, and then re-insert the syringe into the vial to draw up more lidocaine. The practice of this clinic was to reuse lidocaine vials for many different patients until the vial was emptied. The physician realized that by not changing syringes, backwash from the syringe could enter the vial and contaminate the contents.

The physician at the clinic made the difficult decision to alert the risk manager. The hospital began an investigation and included the physician in the process. It determined that none of the biopsied patients had contracted a related communicable disease. However, hospital administrators ultimately decided to disclose the potential exposure to the patients they identified to be at risk. The hospital sent letters to the patients advising them of the possible exposure, apologizing for the mistake and referring them to a hospital contact. To date, there have been no responses from any patients and no reports of related infections due to the multi-use vials.

Nevada lawmakers recently passed laws that address infection control in ambulatory surgical centers (ASCs). ASCs will now have yearly-unannounced inspections that will include a nurse inspector. These new laws add protections for whistleblowers and the power to shut down a facility where patient safety is in question, among other provisions. The GAO issued a report in March, 2009 stressing the need to gather information on health-care associated infections in out-patient facilities. It also calls for periodic random surveys of such facilities.

Although the cases outlined above took place at out-patient facilities, many hospitals face the same type of exposure either at the hospital itself or with hospital owned or operated out-patient centers. Therefore, hospitals should develop a

plan for how to disclose adverse incidents that impact a large number of patients. The large-scale disclosure of adverse events is a challenge and is significantly different from disclosure to an individual patient.

When such an incident occurs, the hospital will need to determine whether there is a need to disclose, and how best to disclose the incident. Several factors including actual or potential harm and reputational risk will need to be considered. The steps to be included in deciding in whether to make a large-scale disclosure are:

- Form an event investigation team consisting of in-house experts whose members can quickly scrutinize the clinical and factual issues of adverse events. This team may be the same group that conducts Sentinel Event investigations. The team should determine whether any other individuals, such as those involved in the incident, will be included as part of the investigation team.
- Check with your attorney to determine how best to conduct the investigation in order to protect it under the discovery laws of your state. The team may need to report to the quality department or general counsel.
- In parallel with the event investigation, the hospital can create a team of professionals from diverse backgrounds (the disclosure team) who will take responsibility for the actual disclosure process. The team should include legal counsel and someone with public relations expertise.
- The hospital may wish to notify its insurance carrier to put it on notice of potential claims and to receive assistance in developing the disclosure plan.
- The disclosure team should decide whether the event should be disclosed. This will depend on:
 - The probability of exposure for each patient; and whether the exposure was of a magnitude to cause harm.
 - Whether there is potential harm to third parties (for example, transmission of



blood borne pathogen to a spouse or significant other).

- Decide whether to disclose by letter, by telephone and/or through the media. Depending on the type of exposure, timely disclosure may be critical.

Once it has been determined that there will be a disclosure, the hospital should develop an internal plan to manage its response to the disclosure:

- Designate one or more contact persons to answer patient calls and questions, press inquiries, and attorney communications. Be sure that they have resources to respond to the expected number of queries and the skills necessary to answer questions and work with angry and emotional patients.
- Develop a plan to provide testing or treatment to those individuals who were exposed. Include

“Done correctly,
a large-scale
disclosure can
help you prevent
lawsuits and
mitigate losses.”

department heads who will be impacted, such as laboratory and phlebotomy.

- Institute a process to insure that patients are not billed for the testing.
- Institute a system to communicate positive test results. Will the patient's primary care physician or the hospital directly discuss these results?
- Ensure that a process through which patients can receive follow-up treatment, if needed, is in place.
- Develop an internal communications plan. Staff should be aware of the incident, what steps the organization has taken, what it plans to do to address the incident and how it will mitigate the risk of it happening again.

Large-scale disclosure must be a well-thought-out process in order to help reassure the potentially harmed patients and help protect the integrity of the organizations. Done correctly, a large-scale disclosure can help you prevent lawsuits and mitigate losses. •

To learn more about Zurich healthcare insurance products and risk management solutions, visit us at www.zurichna.com/healthcare.

Resources

ASHRM Disclosure Laws: State by State www.ashrm.org/ashrm/resources/disclosurelaws.html
ASHRM MONOGRAPH: Disclosure: What works now & What can work even better. Feb 2004
<http://www.ashrm.org/ashrm/resources/files/Disclosure.Part3.0204.pdf>

The Joint Commission Medical Errors Disclosure: Selected Bibliography

www.jointcommission.org/PatientSafety/me_bibliography.htm

Disclosure of Adverse Events to Patients. Department of Veterans Affairs. VHA Directive 2008-02. January 2008.

http://www.ethics.va.gov/ETHICS/docs/policy/VHA_Directive_2008-002_Disclosure_of_Adverse_Events_20080118.pdf

Communication and Disclosure Training Program. ECRI Institute, 2008 May.

<https://members2.ecri.org/Components/PPRM/Pages/EduTrain2.aspx>

CRICO/RMF Disclosure of Unanticipated Outcomes

www.rmfm.harvard.edu/patient-safety-strategies/communication-teamwork/disclosure/disclosure-support-materials.aspx

The information in this article was compiled from sources believed to be reliable for informational purposes only. All sample procedures herein should serve as a guideline that you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this article and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

© 2009 Zurich Services Corporation. All rights reserved.

Contributors

Lee Schmidt is a senior risk consultant for Zurich Healthcare. She is responsible for working with Zurich policyholders to provide consultative education and advice on risk management issues. These include clinical risk assessments, research and in-service educational programs. Lee previously worked at The Clarity Group, providing risk, quality and patient safety services and education to healthcare organizations. She also worked as a risk manager at Sinai Health System, and a claim specialist and risk consultant at CNA Insurance. Lee has been on the faculty of nursing at University of Wisconsin, Milwaukee. She received a BSN from the College of Saint Teresa, a M.S. from University of Illinois at Chicago, and a JD from IIT Chicago-Kent College of Law. Lee is a member of national and several regional ASHRM chapters.

Susan Salpeter is vice president and director of Healthcare Risk Management for Zurich's specialty healthcare business. She is responsible for the management and provision of all healthcare risk management services for Zurich's healthcare professional liability products. Ms. Salpeter was previously risk manager for Loyola University Medical Center, where she was responsible for all loss control activities for a 500-bed teaching hospital, outpatient services, employed physicians and residency program. She is an R.N. and received her bachelor's degree from Washington University, and an MBA from the Kellogg Graduate School of Management with a concentration in Health and Hospital Administration and Finance. Ms. Salpeter is certified by ARM and is a Fellow of the American Society for Healthcare Risk Management.



ZURICH®

One Liberty Plaza
30th Floor
New York, New York
10006

(08/09) 09-2834

Visit us at
ASHRM
Booth 313

