Dexcomm
ANSWERING AND COMMUNICATIONS SERVICES
YOUR VOICE. HEARD.

HIPAA Threats & Breaches

2012

Contents

PLEASE NOTE - Our e-books are designed to provide information about the subject matter covered. It is distributed with the understanding that the authors and the publisher are not engaged in rendering legal, accounting, or other professional services. If legal advice or other professional assistance is required, the services of a competent professional person should be sought.

Our passion is properly serving customers. Operating as a 24/7/365 Telephone Answering Service and Medical Exchange since November of 1954 we have developed skills and techniques that allow us to delight a wide range of clients. As we have grown and prospered for over 50 years we feel now is a great time to give something back to our customers, prospective customers and anyone seeking to improve their business success. Included in this book are tips and tools that we hope will make your job a bit easier each day. One of the great learning tools we have employed is the willingness to learn from our mistakes. Please take advantage of our many years of experience and avoid some of the pitfalls that we have learned to overcome. Our hope is that you and your office can adopt some of these tools to make your life a bit less complicated and allow you a bit more uninterrupted leisure time.

Thanks for listening,

Jamey Hopper
President
Dexcomm

Why Perform a Risk Assessment?

The best answer to this question may be obvious...but it's the law!

Aside from that, there are several good reasons to performing a HIPAA Risk Assessment in your office. A risk assessment can help you to identify where your Protected Health Information (PHI) lies in your organization. From equipment to files, there is PHI being stored everywhere....so, protect yourself. Don't let your office be another case study.

01 Case Study

PHI for Personal Gain

A licensed practical nurse (LPN) pled guilty to wrongfully disclosing a patient's health information for personal gain. The woman faces a maximum of ten (10) years imprisonment, a $250,000 fine or both. Having shared the patient's information with her husband, the husband contacted the patient and told the patient that he was going to use the information against him in an upcoming legal proceeding.

How does this affect me?

02 Case Study

Employees & Facebook

A temporary employee at a California hospital posted a picture of someone's medical record to his Facebook page and made fun of the patient's condition.

Details of the health data breach indicate that the temporary employee, who was provided by a staffing agency, shared a photo on his Facebook page of a medical record displaying a patient's full name and date of admission.

Techniques on preventing a breach

03 Case Study

Fined $100K for Calendar

A five-physician practice became the first small practice to enter into a resolution agreement that included a civil money penalty over charges that it violated the HIPAA Privacy and Security Rules. A complaint was filed alleging that the practice was posting surgery and appointment schedules on an Internet-based calendar that was publicly accessible.

Are you are risk?

How to
Perform a HIPAA Risk Assessment

01 Take Inventory

Take an inventory in your office of equipment like hardware, software, operating systems, operating environment, remotes, removable media, mobile devices and backup media. Does it create, transmit or store e-PHI? If so, it falls under the HIPAA Security Rule and is relevant to this risk assessment.

02 Define Vulnerability

Vulnerability is a flow or weakness in the system which could be exploited. Ask yourself, "is this a threat?" For example, "do vendors or consultants create, receive, maintain transmit e-PHI on behalf of my office? If so, what are the potential threats?" In addition, ask yourself, "What are the human, natural and environmental threats to information systems that contain PHI?"

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

03 Identify Controls

Controls are security systems, firewalls or other regulators that are currently employed to protect PHI from threats.

Certified Health IT Product List

04 Classify Impact

Each threat or vulnerability should be assessed in light of the impact the event would have on PHI and the IT system: loss of confidentiality (unauthorized use or disclosure); loss of integrity of the data (typos or missing information); or a loss of data availability (viruses and malware). Use numeric values, or "low", "medium", "high".

HIPAA—Security considerations
45 C.F.R. § 164.306(b)(2)(iv).

How to
Perform a HIPAA Risk Assessment

05 Identify Risk Level

Compare the likelihood that the threat will be realized or become an event to the level of impact the risk, if realized, will have. Using the same value system when classifying the impact using numeric values, or “low”, “medium”, “high”.

06 Employ Controls

Consider whether the threat or its impact may be reduced or eliminated by employing a control method, such as stronger passwords, security patches, etc. This should also include a cost benefit analysis.

07 Prioritize

Assign a numeric value to designate level of priority. This will help you to achieve risk management based on that level of threat, impact and the availability of controls to reduce or eliminate the risk.

08 Manage

Develop and implement a risk management plan from the Risk Assessment. Implement, maintain and continuously evaluate security measures (controls).

Dexcomm’s Security Checklist

Easy Risk Assessment Template

HIPAA breaches can still happen.

What do HIPAA breaches look like?

- An internal or external party reports a violation
- A review of server logs indicates unauthorized access
- Equipment is reported lost or stolen

01 Case Study

Costly Vendor Mistake

A recent example of this accountability is a lawsuit filled by the Minnesota Attorney General against Accretive Health, Inc., a debt collection agency that is part of a New York private equity fund conglomerate. The agency has a role in managing the revenue and health care delivery systems at two Minnesota hospital systems. In 2011, an Accretive employee lost a laptop computer containing unencrypted health data about patients.

Do your vendors get HIPAA?

02 Case Study

Unauthorized Access

In the spring of 2010, Huping Zhou, a Chinese immigrant living in California, was fined $2,000 and sentenced to four months in prison. He continued to access private medical records through an electronic password-protected database. His previous supervisor, former co-workers and other high-profile celebrity patients were among those whose privacy Zhou violated over a three-week period in 2003.

How does this affect me?

03 Case Study

Where is Your Laptop?

A laptop computer containing patient records went missing from a Louisiana hospital. Information on the laptop contained PHI (protected health information) for 17,130 patients, gathered for a study from 2000 to 2008. A search was initiated as soon as the hospital learned of the disappearance of the missing device, which police are still investigating. The missing laptop has not resur-

Learn about mobile device breaches

What if I discover a breach?

01 Gather Information

Ask who, what, when, where, how. Who was it disclosed to, how was it disclosed, when was it disclosed, etc.

02 Make Contact

Relevant parties may include patients, employees, authorities, media, Secretary of HHS.

03 Define Resolution

In cases where breaches happen, the medical office must communicate steps to prevent them from happening again. The HIPAA Security Rule also requires that you communicate this information to the relevant parties.

04 Document

Document each step you took to resolve the HIPAA breach.

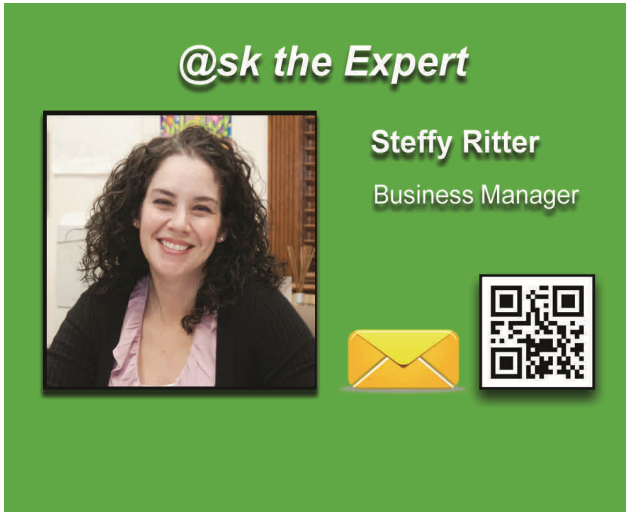
Accounting for Disclosures

Documentation for HIPAA Breaches

Who & When to contact for a breach

Who	When the breach is under 500 records	When the breach is 500 and over
Individual	No later than 60 days from the discovery of the breach, you must notify affected individuals in written form by first-class mail, phone or email	No later than 60 days from the discovery of the breach, you must notify affected individuals in written form by first-class mail, phone or email
Media	Not applicable	No later than 60 days from the discovery of the breach, you must notify prominent media outlets serving your state or jurisdiction
Secretary of HHS	On an annual basis, you must notify the Secretary of Health and Human Services	No later than 60 days from the discovery of the breach, you must notify the Secretary of Health and Human Services
Covered Entity	**If you are a Business Associate:** You must notify the *Covered Entity* no later than 60 days from the discovery of the breach	**If you are a Business Associate:** You must notify the *Covered Entity* no later than 60 days from the discovery of the breach

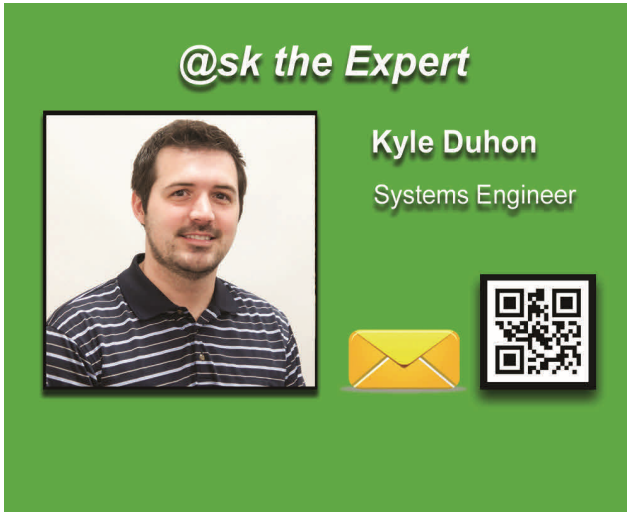
The Dexcomm Difference



Since 1989, before the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Dexcomm focused on and conducted confidentiality training because of our long history and understanding of the medical community we so proudly serve.

We are committed to bring our award-winning service and in-depth knowledge of HIPAA to a new standard of excellence. Dexcomm experts have recently founded and instituted a national certification program for medical operators. This program is designed to develop a superior class of operators, who answer for the medical community, which will change the way our industry serves you.

Visit us at www.dexcomm.com to learn more about the Dexcomm difference.



Administrative Safeguards

- Regular in-house training and instruction of HIPAA and HITECH
- Education provided by a legal HIPAA consultant and RN
- Background checks and regular drug screening of staff
- An expert Security and Privacy Officer
- All employees, visitors and contractors are required to sign confidentiality agreements upon entering

Physical Safeguards

- Password protected access to information and facilities
- Proper destruction of documents and equipment

Technical Safeguards

- Multiple levels of encrypted data backup and security
- Innovative secure messaging systems for mobile devices

Better Business Associates by Design

Connecting Your Practice to the Resources You Need

Conducting HIPAA Risk Assessments to protect your medical office is a must, but ongoing assessments and compliance is vital to ensuring protection.

At Dexcomm, our business associates rely on our services to accurately take and deliver their messages while safeguarding their best interest legally as well as financially. Our Experts are continuously developing complimentary resources tools to assist you in your success.

To find out go to:

dexcomm.com

mybusinessheard.com

dexcomm.com/ resources

@sk the Expert

Dexcomm
877.339.2666
Corporate: 518 Patin Rd. Carencro, LA 70520

Interested in Dexcomm's services?

Get a Quote

READY TO GET STARTED?

Click Here to Begin.