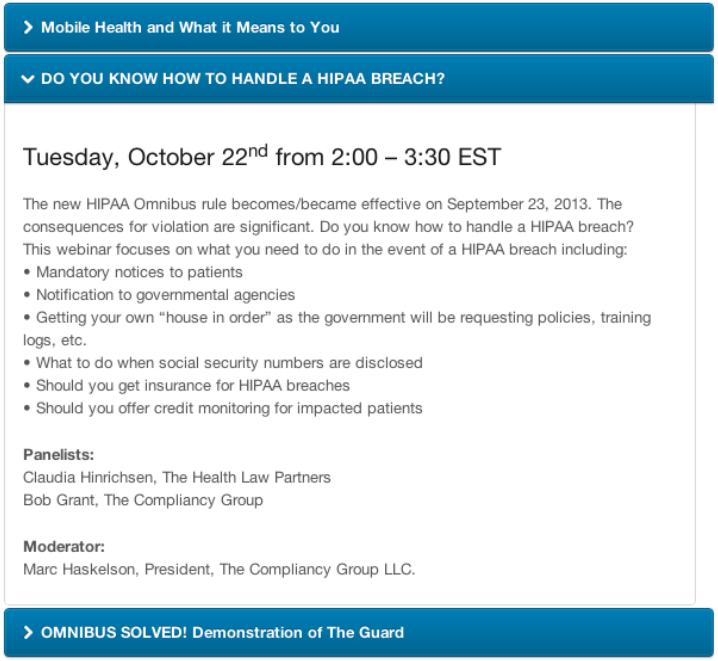
Do You Know How To Handle A HIPAA Breach?

Claudia A. Hinrichsen, Esq.
The Greenberg, Dresevic, Hinrichsen, Iwrey, Kalmowitz, Lebow & Pendleton Law Group
(516) 492-3390
chinrichsen@thehlp.com

Achieve.Illustrate.Maintain.

Compliance *Simplified*

Industry leading Education



- **Please ask questions**
- **For todays Slides**

http://compliancy-group.com/slides023/

- **Todays & Past webinars go to:**

http://compliancy-group.com/webinar/

Join our chat on Twitter

#cgwebinar

Compliancy Group

Agenda

I. Definition of Breach and Risk Assessment
II. Notification obligations in event of HIPAA breach
III. Getting you own “house in order”
IV. What to do when social security numbers are disclosed
V. Credit monitoring for impacted patients
VI. Insurance for HIPAA breaches
VII. Questions?

HIPAA Omnibus Rule

- New HIPAA regulations became effective on September 23, 2013
- Significant modifications made to HIPAA rules, including breach notification, among other things
  - Harm standard removed
  - Four factors must be considered in risk assessment

Determine Whether a Breach Occurred

- Impermissible use or disclosure of protected health information (PHI) is presumed to be a breach unless the Covered Entity is able to demonstrate that there is "l*ow probability that PHI has been compromised*."
  - Applies to "unsecured PHI" which is not rendered unusable, unreadable, or indecipherable

Determine Whether a Breach Occurred

At least the four following factors must be assessed:

1) The *nature and extent* of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2) The *unauthorized person* who used the PHI or to whom the disclosure was made;
3) whether the PHI was *actually acquired or viewed*; and
4) The extent to which the risk to the PHI has been *mitigated.*

Results of Risk Assessment

- If evaluation of the factors fails to demonstrate that low probability that the PHI has been compromised, *breach notification is required.*

Example 1

- If information containing dates of health care service and diagnosis of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on the information available to the employer, such as dates of absence from work.
  - In this case, there may be more than a low probability that the protected health information has been compromised.

Example 2

- If a laptop computer was stolen and later recovered and a forensic analysis shows that the protected health information on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the Covered Entity could determine that the information was not actually an unauthorized individual even though the opportunity existed.

Example 3

- If financial information, such as credit card numbers or social security numbers was disclosed, the Covered Entity may determine that a breach has occurred as unauthorized use or disclosure of such information could increase the risk of identity theft or financial fraud.

Notification Obligations in the Event of a HIPAA Breach

- Notification to affected individuals
- Notification to the media
- Notification to the Secretary of the Department of Health and Human Services (the Secretary)
- Other notifications

Notification to Affected Individuals

- All notices to affected individuals must be written in plain language and include:
  - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  - A description of the ***types*** of PHI (not the specific PHI) that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

Notification to Affected Individuals

- Any recommended steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the Covered Entity is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches; and
- Contact information for the Privacy Officer of the Covered Entity.

Method of Notification

- The covered entity must notify affected individuals by:
  1. Written notification by first-class mail to the individual at the last known address of the individual
  2. If the individual agrees to electronic notice and such agreement has not been withdr

Method of Notification

- In the case of minors or individuals who lack legal capacity due to a mental or physical condition, the parent or personal representative should be notified.
- If the covered entity knows that an individual is deceased, the notification should be sent to the individual's next of kin or personal representative if the address is known.

Method of Notification

- In urgent situations where there is a possibility for imminent misuse of the unsecured PHI, additional notice by telephone or other means may be made. However, direct written notice must still be provided.

Notification to the Media

- If the breach of unsecured PHI involves more than 500 residents of a state or jurisdiction, prominent media outlet must be notified (most likely via a press release) without unreasonable delay and no later than 60 days after discovery.

PLEASE NOTE: The notification to the media is not a substitute for the notification to the individual.

Notification to the Secretary

- For breach of unsecured PHI that involves *more than 500 individuals*, the Secretary of the Department of Health and Human Services should be notified via ocrnotifications.hhs.gov without unreasonable delay and *no later than 60 days after discovery*.

Notification to the Secretary

- If the breach of unsecured PHI involve less than 500 individuals, the Covered Entity's Privacy Officer should maintain an internal log or other documentation of the breach. This information should then be submitted annually (before March 1st) to the Secretary of HHS for the preceding calendar year via the website.
  - The health care provider should maintain its internal log or other documentation of breaches for six years.

Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information

Breach Affecting

○ 500 or More Individuals ○ Less Than 500 Individuals

Report Type

○ Initial Breach Report ○ Addendum to Previous Report

Section 1 - Covered Entity

Name of Covered Entity: John Doe

Address: Line 1

Line 2

City: City

State: AL **Zipcode:** XXXXX

Contact Name: John Doe

Contact Phone Number:
XXX-XXX-XXXX XXX-XXX-XXXX

Contact E-mail: example@example.com

Type of Covered Entity: Health Plan

Section 2 - Business Associate

Complete this section if breach occurred at or by a Business Associate

Name of Business Associate: John Doe

Address: Line 1

Line 2

City: City

State: AL **Zipcode:** XXXXX

Business Associate Contact Name: John Doe

Business Associate Contact Phone Number:
XXX-XXX-XXXX XXX-XXX-XXXX

Business Associate Contact E-mail: example@example.com

Section 3 - Breach

Date(s) of Breach:
MM/DD/YYYY (- MM/DD/YYYY)

mm/dd/yyyy - mm/dd/yyyy

Date(s) of Discovery:
MM/DD/YYYY (- MM/DD/YYYY)

mm/dd/yyyy - mm/dd/yyyy

Approximate Number of Individuals Affected by the Breach:

Type of Breach:
Please select the type of breach. If type breach is "Other", please describe the type of breach in the field below.

- [ ] Theft
- [ ] Loss
- [ ] Improper Disposal
- [ ] Unauthorized Access/Disclosure
- [ ] Hacking/IT Incident
- [ ] Unknown
- [ ] Other

Type of Breach (Other):

Location of Breached Information:
Please select the location of the information at the time of the breach. If breach type is "Other", please describe the location of the information in more detail in the Description section below.

- Laptop
- Desktop Computer
- Network Server
- E-mail
- Other Portable Electronic Device
- Other

Type of Protected Health Information Involved in the Breach:

- Demographic Information
- Financial Information
- Clinical Information
- Other

Brief Description of the Breach:
Please include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach.

Section 4 - Notice of Breach and Actions Taken

Date(s) Individual Notice Provided:
MM/DD/YYYY (- MM/DD/YYYY)

mm/dd/yyyy - mm/dd/yyyy

Was Substitute Notice Required?

○ Yes ◉ No

Was Media Notice Required?

○ Yes ◉ No

Actions Taken in Response to Breach:
Please select the actions taken to respond to the breach. If selecting the "Other" category, please describe the actions taken in the section below.

Security and/or Privacy Safeguards
Mitigation
Sanctions
Policies and Procedures
Other

Describe Other Actions Taken:
Please describe in detail any actions taken following the breach in addition to those selected above.

Section 5 - Attestation

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

Name: Full Name
Typing your name represents your signature

Date: mm/dd/yyyy
MM/DD/YYYY

Submit

Getting Your "House in Order"

- Review/update the practice's *policies and procedures*
- Provide *training* to all employees in:
  - Updated policies
  - Prompt reporting
  - Evaluation and documentation of breaches
- Create an *action plan* to respond to security incidents and breaches
- Conduct regular *internal audits*
- Consider getting *insurance* for HIPAA breaches

Most Common Forms of Breach

- **Impermissible uses and disclosures** of protected health information
- **Lack of safeguards** of protected health information
- **Lack of patient access** to their protected health information
- Uses or disclosures of more than the **Minimum Necessary** protected health information
- **Complaints** to the covered entity

Office of Civil Rights (OCR) Audits

- OCR has completed audits for 115 entities with a total of 979 audit findings and observations:
  - 293 regarding Privacy
  - 592 regarding Security
  - *94 regarding Breach Notification*
- An evaluation is currently underway to make audits a permanent part of enforcement efforts.
- Security Rule assessment will be highly scrutinized.

Social Security Numbers

- Most states have additional laws regulating notification of unauthorized disclosure of social security numbers.
  - These regulations require that notification be provided in the most expeditious time possible and without unreasonable delay.
  - The person that owns or licenses the computerized data must provide notice to the individual.

Social Security Number Breach

- Typically the following must be done immediately after discovery of the breach:
  - Detailed notice to affected residents within state
  - Notification to other governmental agencies, including, but not limited to:
    - State Attorney General
    - Department of State
    - Consumer Reporting Agencies

PLEASE NOTE: The Attorney General may bring a civil action and the court may also award injunctive relief.

Credit-Monitoring

- According to the U.S. Federal Trade Commission, it takes an average of 12 months for a victim of identity theft to notice the crime.
  - Credit-monitoring services will regularly alert the individual of any changes to their credit, helping stop theft before it gets out of control.

Credit-Monitoring

- Covered entities and others who maintain PHI may need to offer such services to affected individuals to mitigate risk.
  - Companies such as Identity Guard, Equifax, and Experian offer credit-monitoring, providing credit alerts to individuals every business day.
  - The average cost of credit monitoring per person is $15 a month with credit alerts which will report new accounts, credit inquiries, address changes, changes to current accounts/account information, etc.

Business Associate Agreements

- Covered Entities should include indemnification language in their Business Associate Agreement for any costs related to a breach including free credit-monitoring for affected individuals.
  - A Covered Entity may also consider requiring business associates to have data breach insurance.

Cyber/Breach Insurance

- A recent study by the Ponemon Institute reported that 76% of participating organizations in the study who had experienced a security exploit ranked cyber security risks as high or higher than other insurable risks, such as natural disasters, business interruptions, and fire.
  - Many general liability insurance polices are excluding data breaches ad security compromises.

Cyber/Breach Insurance

- Data breach insurance may be necessary to cover the costs of responding to a breach and may include:
  - Defense costs and indemnity for a statutory violation, regulatory investigation, negligence or breach of contract
  - Credit or identity costs as part of a covered liability judgment, award or settlement
  - Forensic costs incurred in the defense of covered claim

Conclusion

- "Thus far in 2013, 48 percent of reported data breaches in the United States have been in the medical/healthcare industry. In 2012, there were 154 breaches in the medical and healthcare sector, accounting for 34.5 percent of all breaches in 2012, and 2,237,873 total records lost."
  - ITRC Breach Report, Identity Theft Resource Center, May 2013
- A plan of action is crucial in order to appropriately handle a breach.
  - Proper and timely notification is necessary

Achieve.Illustrate.Maintain.

Compliance *Simplified*

- ✓ HIPAA Compliance
- ✓ HITECH Attestation
- ✓ Risk Assessment
- ✓ Omnibus Rule Ready
- ✓ Meaningful Use core measure 15
- ✓ Policy & Procedure Templates

Free Demo and 60 Day Evaluation

www.compliancy-group.com

HIPAA Hotline

855.85HIPAA

855.854.4722

Compliancy Group

Questions?