

**DuaneMorris**

**Privacy Issues and the Increasing Use of Information Technology: HIPAA and HITECH**  
(How to Help Your Clients Be Compliant Now and In The Future)

Pennsylvania Bar Institute  
November 15, 2011  
Lisa W. Clark, Esq.

©2011 Duane Morris LLP. All Rights Reserved. Duane Morris is a registered service mark of Duane Morris LLP.  
Duane Morris - Firm and Affiliate Offices: New York | London | Singapore | Los Angeles | Chicago | Houston | Miami | Philadelphia | San Diego | San Francisco | Baltimore | Boston | Washington, D.C.  
Los Vegas | Atlanta | Miami | Pittsburgh | Newark | Boca Raton | Wilmington | Cherry Hill | Lake Tahoe | No. Cox Minn City | Duane Morris LLP - A Delaware limited liability partnership

[www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

---

---

**DuaneMorris**

HIPAA/SECURITY TRAINING  
 IF A GOVT ATE A COPY OF THESE REGULATIONS MANUAL WOULD WOULD BE THE ONLY  
 • ANTI-DEFISATIONS  
 • FIDUCIARY  
 • RESISTANT-SECURSION  
 • CONSIDERING PENALTION CRIMES

"We need to review our training material."

2 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

---

---

**DuaneMorris**

**Overview of Presentation**

1. *Background on HIPAA/HITECH (the basics\*)*
  - What are HIPAA and HITECH?
  - Who is subject to HIPAA/HITECH?
  - What information does HIPAA/HITECH apply to?
  - What other laws apply?
  - What information is protected under HIPAA and other laws?
2. *Healthcare's (forced) embrace of technology.*
3. *Client Priority Issues ## 1-11 - to help your client implement HIPAA and HITECH.*

\* See handout materials for detail on HIPAA and HITECH

3 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

---

---

DuaneMorris

Federal Laws

- 1. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"):**
  - Privacy and security protections for PHI
  - Data breach notification requirements
- 2. Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009**
  - Amended HIPAA to make it stricter

4 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris



©Cartoonbank.com

©Cartoonbank.com

© 2009

*"It's a baby. Federal regulations prohibit our mentioning its race, age, or gender."*

www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Three Main Rules under HIPAA

- **Privacy Rule** – applies to ALL PHI
- **Security Rule** – applies to electronic PHI only
- **Data Breach Rule** – applies to all PHI breaches; *mandatory* reporting

6 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

### New Enforcement Era

HITECH added new enforcement penalties:

- \$100-\$50k for single violation (up to \$1.5k for identical violations in single year)
  - > Penalty tiers based on
    - what you knew about the violation
    - what you should have known, and
    - how quickly you acted to correct it

7 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

### New Enforcement Era

- Degree of enforcement against Provider (including penalties and corrective action) will also depend on Covered Entity's response to violations, ***including actions taken against employees.***
- Caution: Serious violations can be subject to criminal action. A UCLA nurse was jailed under HIPAA's criminal enforcement provisions for improperly accessing records

8 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

### HIPAA Background/Who is subject to HIPAA

a. "Covered Entities"

1. Health Care Providers who engage in HIPAA-defined electronic transactions.
2. Health Plans such as Medicare, Medicaid, commercial plans.
  - i. Includes Group Health Plans – employee health benefit programs
3. Health Care Clearinghouses such as billing companies

b. Business Associates – subcontractors who provide business support services to HIPAA-Covered Entities

1. Subcontractors to BAs also have responsibilities.

9 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**HIPAA Background/Who is subject to HIPAA, cont.**

d. So in terms of clients, just who is subject to HIPAA?

- i. Most health care providers, including small providers such as behavioral health/mental health/community health facilities and individual practitioners
- ii. Clearinghouses
- iii. Provider group health plans (not a separate legal entity, usually the HR Department)
- iv. Business Associates – those who perform business services on your behalf, e.g., billing companies, data analysts, lawyers
- v. Health Plans.

10 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**HIPAA Background/What is Protected?**

a. PHI

- i. Any patient-identifying information
- ii. Psychotherapy notes specifically protected

b. Goes by other names under other laws

- i. For d&a providers, "patient identifying information"

11 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**HIPAA Background/Where is PHI located?**

- a. On paper
- b. Verbally
- c. Electronically
  - i. Legacy electronic systems
  - ii. Electronic health records (EHRs)

12 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Other sensitive information covered by other laws

- Substance abuse
  - Drug and Alcohol Treatment Confidentiality Regulations (42 C.F.R. Part 2)
  - State substance abuse privacy laws
- Mental health (state) laws
- HIV-AIDS (state) laws
- Reproductive health (federal and state) laws
- Genetic testing (federal and state) laws

13 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Special Laws governing sensitive health care information

- These Special Laws are often stricter than HIPAA.
- No specific laws for community health centers or providers treating developmentally disabled. But HIPAA, Part 2, and state laws may apply!

14 www.duanemorris.com

---

---

---

---


---

---

---

---

DuaneMorris



15 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

### Background/Overview of Legal Developments

1. HIPAA amended by the HITECH Act of 2009 (part of ARRA of 2009)
2. ARRA provided monies for certain health care providers to stimulate health information technology ("HIT") through
  - a. Adoption of EHRs.
  - b. Development of private and secure health information exchange.

16 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

### EHR Technology/Meaningful Use

3. Under ARRA, hospital and some health care professionals must be "Meaningful Users" of EHR technology to receive incentive payments. This means:
  - Using certified EHR systems that meets certain criteria, such as e-prescribing.
  - Engaging in the electronic exchange of health information
  - Using EHR technology to submit clinical quality and other measures.

17 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

### HIT and Behavioral Health

- The EHR incentives do not extend to most behavioral health entities and professionals.
- Behavioral Health Information Technology Act of 2011 introduced to expand incentive programs to
  - Community mental health centers, mental health treatment facilities, psychiatric hospitals and substance abuse treatment facilities.
  - Licensed psychologists and social workers.

18 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

### HIT and Behavioral Health/What's it like now?

- Twenty percent of 175 substance abuse treatment programs surveyed had no information systems, e-mail or even voice mail.
- On average, IT spending in behavioral health care/human services organizations represents 1.8 percent of total operating budgets—compared with 3.5 percent of the total operating budgets for general health care services.
- Fewer than half of behavioral health and human services providers possess fully implemented clinical electronic record systems.
- State and Territorial laws vary on the extent that providers can share medically sensitive information such as HIV status, treatment for psychiatric conditions or rules on sharing medical data.
- A study of 56 mental health clinicians in an academic medical center revealed that their concerns regarding privacy and data security were significant, and may contribute to the reluctance to adopt electronic records.  
<http://www.samhsa.gov/about/157AdministratorHandoutSI.pdf>, p. 10

19 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

### Other HIT Developments

- a. Health information organizations (HIOs) – exchanges developed to share information
- b. Telemedicine/cybermedicine
- c. Personal health records (PHRs) – may or may not be tethered to EHRs

20 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

### Other HIT Developments

- d. If this all wasn't enough, don't forget increasing number of innovative products and services to support health care delivery (usually in IT arena)
  - i. Tools to help individuals monitor health
  - ii. Data mining tools for quality, payment purposes
  - iii. Social media

21 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

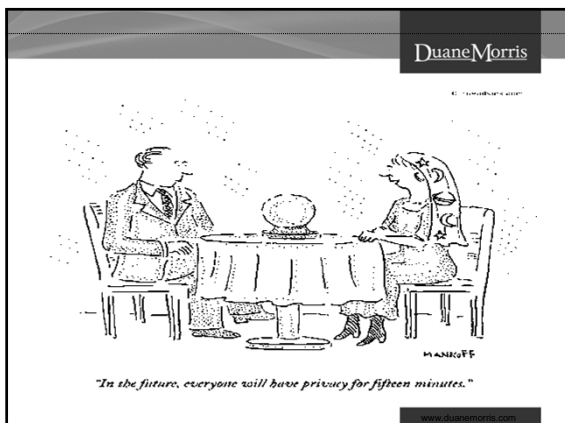
---

---

---

---

---



---

---

---

---

---

---

---

---

DuaneMorris

So What May Your Client Be Doing To Become Compliant and What Can You Do?

- *If a provider, possible adoption of EHR system*
  - May or may not be certified
- *Possible consideration of HIO participation*
- *Likely awareness of privacy issues due to HIPAA*
- *HIPAA program?*
  - May or may not be comprehensive
  - All workforce members may or may not have been trained
  - Clearinghouses and BAs may not have program.
- *Expensive!!*

23  
www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Client Priority Issue #1: Focus on Your Security Program

a. Questions to ask:

- i. What does your Security Program look like?
- ii. Have you adopted an EHR program?
- iii. Are you considering participating in an HIO?
- iv. Have you identified your subcontractors who handle PHI?

24  
www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #1: Focus on Your Security Program, cont.**

**b. Security Program**

- i. HIPAA Security Rules requires Covered Entities to comply with Security Standards, e.g., access, audit, etc.
- ii. HHS has helpful guidance on complying with Security Rule.  
[www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html)

25 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #1: Focus on Your Security Program, cont.**

**c. EHR adoption**

- i. EHR will vary based on type of providers.
- ii. Tricky because state of the law.
- iii. Work with knowledgeable IT consultant – grill on HIPAA understanding for behavioral health providers!!!! Ask about ability to interconnect with other systems, ability to modify, etc.

26 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #1: Focus on Your Security Program, cont.**

**d. Think about your subcontractors....**

- i. Do they handle PHI?
- ii. Consider all of the various subcontractors that impact your Security Program, e.g.,
  - a. IT consultants
  - b. Billing entities
  - c. Janitors

27 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Client Priority Issue #1: Focus on Your Security Program, cont.

- RANDOM SECURITY AUDITS ARE COMING LATE 2011-EARLY 2012!!!!!!

28 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Client Priority Issue #2: Review Your Privacy Program

- Most Covered Entities have a Privacy Program...but is it up-to-date?
  - How long has it been since staff was trained, policies, reviewed, etc.?

www.duanemorris.com

---

---

---

---


---

---

---

---

DuaneMorris



*"Normally, I'd discuss your condition with these first-year residents, but because of confidentiality restrictions, all I can really tell them is that you're a show-in for an invasive procedure."*

30 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #2: Review Your Privacy Program, cont.**

- The HIPAA Privacy Rule's administrative requirements are:
  - Privacy official
  - Contact person for complaints
  - Training
  - Safeguards
  - Complaints
  - Sanctions
  - Mitigation
  - Intimidating or retaliatory acts
  - No waiver of rights
  - Policies and procedures
  - Documentation

31 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #3: Business Associates (BAs) and BA Agreements**

- a. Your subcontractors that handle PHI are your Business Associates
  - i. Anyone who "steps in your shoes" to perform a business function
- b. If you are covered by Part 2, BAs are called Qualified Service Organizations
  - i. QSOs include labs and other treatment providers (different from HIPAA)

32 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #3: Business Associates, cont'd**

- a. Must have written Business Associate Agreement in place
- b. Business Associates are now subject to HIPAA penalties for HIPAA security and other violations
- c. Read your contracts carefully – should include tight and precise breach notice time frame (e.g, 5 days) !!!

33 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

DuaneMorris



*"I said we have to educate our business associates, then hit them with the contract, but not physically."*

34 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

**Client Priority Issue #3: Business Associates, cont'd**

- Business Associates also include third parties that exchange PHI with Covered Entities including:

- Personal health records (PHR) vendors;
- Health information exchange organizations; and
- Regional health information organizations.

35 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

**Client Priority Issue #3: Business Associates, cont'd**

"A medical privacy breach led to the public posting on a commercial Web site of data for 20,000 emergency room patients at Stanford Hospital in Palo Alto, Calif., including names and diagnosis codes, the hospital has confirmed. The information stayed online for nearly a year. Since discovering the breach last month, the hospital has been investigating how a detailed spreadsheet made its way from one of its vendors, a billing contractor [I.E., A BUSINESS ASSOCIATE] identified as Multi-Specialty Collection Services, to a Web site called Student of Fortune, which allows students to solicit paid assistance with their schoolwork."

[www.nytimes.com/2011/09/09/us/09breach.html? r=2&hp](http://www.nytimes.com/2011/09/09/us/09breach.html? r=2&hp)

36 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #4: Breach Notification Requirements**

- a. The Breach Notification Rule is HIPAA's newest rule, added under HITECH
- b. Breach reporting is mandatory except if data is "secured"
  - i. Secured data is defined specifically by HHS <http://edocket.access.gpo.gov/2009/pdf/E9-9512.pdf>
- c. Must report to individuals and in some cases to HHS within 60 days of discovery of "breach"

37 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #4: Breach Notification Requirements, cont.**

- d. Breach determined based on risk assessment
- e. In addition to "securing" PHI, consider monitoring data transfer on the drives using back-end management software and creating an audit trail (all part of a strong Security Program)
- f. Breach response is astoundingly expensive (\$\$\$\$) – just ask me.....

38 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #5: The Individual's Rights – and You are Responsible for Compliance**

- a. HIPAA is a civil rights law. Individuals are granted rights including
  - i. Notice
  - ii. Authorization/Consent
    - 1. Be clear on when authorization/consent is required based on the laws that apply to you, e.g., Part 2 requires consent more often than HIPAA
  - iii. Accounting
    - 1. Proposed new rule would give individual right to know which workforce members accessed records.

39 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

Client Priority Issue #5: The Individual's Rights – and You are Responsible for Compliance, cont.

Individual has rights to...

- iii. Amendment
- iv. Access

**STRICT TIME FRAMES APPLY!!!!**

Government does not look fondly on tardiness....

40 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**



*"I know about patient confidentiality, but I have to ask these questions about your medical history. Please stop taking the 5th ..."*

41 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

Client Priority Issue #6: Strict Enforcement of Use and Disclosure of PHI for Sales or Marketing Purposes

- a. No communication to encourage recipient to purchase or use a product or service without written authorization unless communication:
  - i. Describes a health-related product or service provided under a plan of benefits
  - ii. Is made for treatment purposes
  - iii. Is made for case management or case coordination, or to direct or recommend alternative treatments, therapies, providers or settings of care

42 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

Client Priority Issue #6: Strict Enforcement of Use and Disclosure of PHI for Sales or Marketing Purposes, cont.

- b. May not receive remuneration for any communication, without authorization, except
  - i. If communication describes drug currently being prescribed or communication is made by BA
  - ii. If opt-out provision is provided in the Notice

43 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

Client Priority Issue #7: EHRs

- a. If you use an EHR, can you protect against workforce members accessing PHI for the wrong reasons?
  - i. Should be separate fields for sensitive information, e.g., psychotherapy notes
  - ii. Should be warning pages to guard against inappropriate access (the source of most violations)

44 www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

Client Priority Issue #7: EHRs, cont.

- b. With an EHR,
  - i. Seek to separate behavioral health from non-behavioral health PHI to greatest extent possible
  - ii. Employ strong training program
  - iii. Enforce violations!

***Consider that UCLA's employee was jailed for inappropriately accessing celebrities' files, and UCLA paid fine of close to \$1m for lax practices.***

45 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris



"You can't just walk in and ask to access patient records. HIPAA would call that fantasizing."

46 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

### Client Priority Issue #8: HIOs

- c. If you are considering an HIO, discuss with the vendor
  - i. What data will be shared
  - ii. How access will be managed and inappropriate access prevented
  - iii. How to obtain patient consent
  - iv. How breaches will be addressed

**\* Even if you use a recognized (state-based, government funded, etc.) HIO, a breach will affect you – the data belongs to your patients and you are the covered entity!**

47 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

### Client Priority Issue #9: Mobile Devices

- Whenever possible, don't store sensitive data on wireless devices.
- Ensure that data is encrypted when HIPAA requires doing so.
  - Encryption also provides a safe harbor under the HITECH Act. This means the data is considered secure and notifying individuals is unnecessary if the device is lost or stolen:
- Enable password protection on wireless devices, and configure the lock screen to appear after a brief period of inactivity.
- Activate the remote wipe feature of wireless devices that contain personal information.
- Consider IT security features such as using Wi-Fi Protected Access – 2, changing the default service set identifier and administrative passwords and implementing wireless intrusion system.

www.duanemorris.com

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #10: Other Considerations**

1. If law enforcement comes knocking, you can provide PHI subject to applicable law and circumstances.
  - a. Need to know basis.
2. If subpoena arrives requesting PHI, consider applicable law and circumstances.
  - a. Was patient notified?
  - b. Does law require court order as well? (see Part 2)

49 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---


---

---

---

---

**DuaneMorris**



50 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

**DuaneMorris**

**Client Priority Issue #11: Heightened Enforcement**

**HITECH added new enforcement penalties:**

- \$100-\$50k for single violation (up to \$1.5k for identical violations in single year)
  - > Penalty tiers based on
    - what you knew about the violation
    - what you should have known, and
    - how quickly you acted to correct it

51 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

DuaneMorris

Client Priority Issue #11: Heightened Enforcement, cont'd

- No private right of action.
- But, individuals can (and do) use constitution, state laws, to file privacy actions.

52 www.duanemorris.com

---

---

---

---


---

---

---

---

DuaneMorris



*"A lack of privacy and confidentiality suit was filed today by a lawyer representing three white mice from a research lab."*

53 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Client Priority Issue #12: Consider Buying Insurance to Protect Against HIPAA Violations and Breaches

- Although enforcers are supposed to take the size of the organization into account, some of the worst breaches occur at the smaller organizations
- Breach clean-up can run into the hundreds of thousands of dollars

54 www.duanemorris.com

---

---

---

---

---

---

---

---

DuaneMorris

Client Priority Issue #13: Build on the Good Job You're Doing Already! – Next Steps

- Be responsible but don't succumb to HIPAA mania and over-reaction!
- But . . .

55 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

DuaneMorris

Client Priority Issue #13: Build on the Good Job You're Doing Already! - Next Steps, cont.

- Prepare for a government audit:
  - Review P&Ps to ensure they are up to date and comprehensive.
  - Review your files and documentation to ensure that appropriate patient information safeguards exist (e.g., Notice, rights of access, etc.)
  - Review your risk analysis process, risk management plan, incident response plan, emergency backup plan (if any), and breach response plan.
  - Conduct regular internal audits.
  - Assess the overall effectiveness of your entity's approach to privacy and security – demonstrate a culture of compliance
    - > Regular review of P&Ps
    - > Regular training sessions for staff members
    - > Up-to-date plan for prompt response to incidents

56 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---


---

---

---

---

DuaneMorris



57 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---

---

DuaneMorris

**THANK YOU!**

58 [www.duanemorris.com](http://www.duanemorris.com)

---

---

---

---

---

---

---