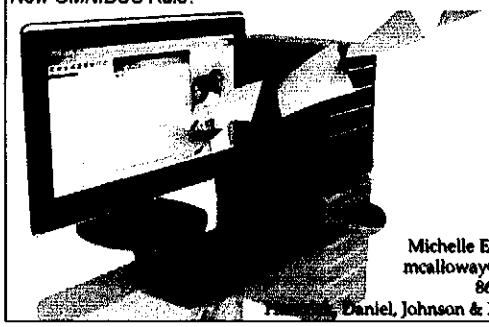
OCR is Headed to a Practice Near You:

Are You Compliant with HIPAA, the HITECH Act and the New OMNIBUS Rule?



Michelle E. Calloway
mcalloway@hdjn.com
866.967.9604
Daniel, Johnson & Nagle, P.C.

Today's Presentation

1. Know the Rules
2. Perform a Risk Assessment
3. Audit Compliance
4. Implement Corrective Action
5. Be Prepared

2 HDJN

1. Know the Rules

- HIPAA
  - **Privacy Rule**: establishes patient privacy rights and addresses the use and disclosure of PHI
    - Mandatory/Permissible Disclosures
    - Authorization
    - Minimum Necessary
    - Notice of Privacy Practices

3 HDJN

1. Know the Rules

- HIPAA
  - **Security Rule**: establishes requirements for protecting electronic PHI
    - Confidentiality / Integrity/ Availability
    - Physical / Technical / Administrative Safeguards
    - Develop and maintain policies and procedures
    - Back up / disaster recovery / emergency plans
    - Risk Assessment
    - Record incidents

4 HDJN

1. Know the Rules

- HIPAA
  - **Breach Notification Rule** unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the information
    - Pre-OMNIBUS Rule: harm analysis
    - Notice to:
      - Affected individual
      - HHS
      - Media
      - Website

5 HDJN

1. Know the Rules

- The HITECH Act
  - Business Associates Liable
  - Accounting of Disclosures
  - Increased Penalties
  - Increased Enforcement
    - Increased Investigations
    - OCR Audits

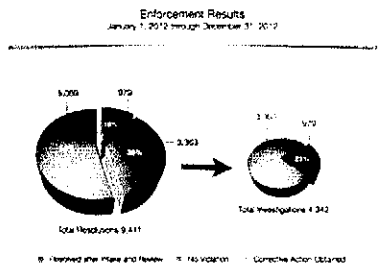
6 HDJN

HITECH Civil Monetary Penalties

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did Not Know	$100-$50,000	$1,500,000
Reasonable Cause	$1,000-$50,000	$1,500,000
Willful Neglect – corrected in 30 days	$10,000-$50,000	$1,500,000
Willful Neglect – not corrected	$50,000	$1,500,000

7 HDJN

OCR Investigations / Enforcement



8 HDJN

OCR Audit Program

- Previously, HIPAA compliance audits only in response to a complaint or breach report
- HITECH Act requires periodic auditing of entities
- $9.2 million to KPMG to perform 150 audits in 2012
- OCR is in the process of evaluating success of audit program – scheduled completion Fall 2013
- Audits likely to re-commence in 2014
- Audit protocol available on OCR website

9 HDJN

1. Know the Rules

- The OMNIBUS Rule
  - Presumption of Breach
  - Updates to Notice of Privacy Practices
  - Updates to Business Associate Agreements
  - PHI of Decedents
  - Immunization Records
  - Research Authorization
- Effective March 16, 2013; mandatory compliance by September 23, 2013

10 HDJN

2. Perform a HIPAA Risk Assessment

- Most common entities required to take corrective action (in order of frequency):
  - Private Practices;
  - General Hospitals;
  - Outpatient Facilities;
  - Health Plans (group health plans and health insurance issuers); and,
  - Pharmacies.

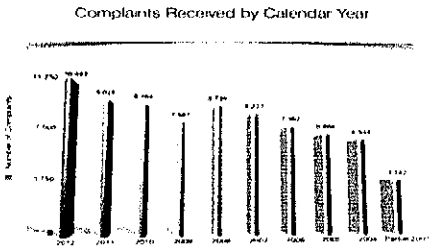
11 HDJN

2. Perform a HIPAA Risk Assessment

- Top 5 Privacy Issues Identified by OCR:
  1. Impermissible uses and disclosures
  2. Insufficient safeguards of PHI
  3. Failure to provide patient access to PHI
  4. Use/disclosure of more than minimum necessary PHI
  5. Insufficient notice to patients of use/disclosure of PHI

12 HDJN

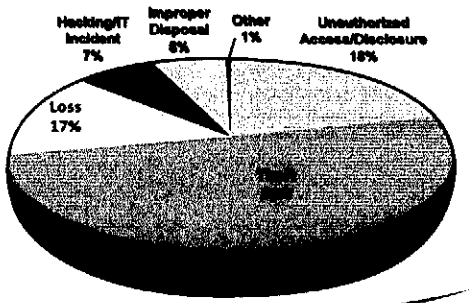
OCR Complaints



13

HDJN

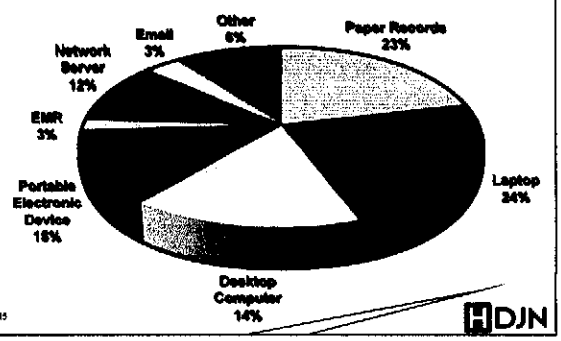
OCR Privacy Issues



14

HDJN

OCR Privacy Issues



15

HDJN

3. Audit Compliance

- For Example:
  - Review HIPAA Privacy & Security Policies and Procedures
  - Review Notice of Privacy Practices
  - Review Business Associate Agreements
  - Encryption Utilization
  - Workstation security
  - Run Access Reports
  - Verify/Update Fax Numbers

16

HDJN

4. Implement Corrective Action

- Stop Inappropriate Conduct
- Perform Breach Analysis
- Breach Notification (if appropriate)
- Revise Policies
- Re-Train
- Discipline (if appropriate)
- Document corrective actions taken

17

HDJN

Recent Enforcement Examples

- **Rite Aid (July 27, 2010)**
  - Improper disposal of prescriptions and pill bottles
  - $1m settlement, CAP, regular training for employees
- **Massachusetts General (February, 2011)**
  - Employee took billing encounter forms home; 192 paper records lost
  - OCR settlement for $1 million, 3 year CAP
- **Phoenix Cardiac Surgery (April, 2012)**
  - Posted clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible.
  - Practice implemented few policies and procedures and had limited safeguards in place to protect patients' electronic protected health information.
  - OCR settlement for $100,000

18

HDJN

5. Be Prepared

- Preparation is Key!
  - Know the rules
  - Perform a Risk Assessment
  - Identify weaknesses and implement corrective measures
  - Ensure staff is effectively trained
  - Conduct fire drills (Internal Audits)
  - Document your efforts
  - Know what OCR is looking for (Protocol Review)

19

HDJN

QUESTIONS

Michelle E. Calloway
mcalloway@hdjn.com
866.967.9604
Hancock, Daniel, Johnson & Nagle, P.C.

26

HDJN