CONVENTUS

HIPAA and Billing Compliance Plan: How to Avoid Audits and Fines

Wiks Moffat, CHC
Principal–Executive Vice President of Compliance
Healthcare Compliance Network

March 30, 2016

CONVENTUS 900 Route 9 North, Ste. 503, Woodbridge, NJ 07095-1003
Website: www.conventusnj.com

1

CONVENTUS

Technical Assistance

- Technical Assistance Telephone Number
  - 732-822-9948
- Question Submission for Q&A Session
  - Type your question into the Questions Box on the control panel on your screen

(PLEASE JOT DOWN THIS INFORMATION)

2

CONVENTUS

Conventus Practice Resources

- Webinars and Podcasts
- Education
  - C.A.R.E. Certification Program – Modules I & II
- Practice Advice Hotline
  - 24/7
- Publications
  - e-News
  - Risk Alerts
  - Practice Success Tips

3

CONVENTUS

Conventus Practice Resources

- Consulting Services
  - Practice Success Consultation & Plan
  - Practice Transformation and Quality Reporting Initiatives
  - EHR Consultation
  - Risk Assessment
- Strategic Partnerships
  - HIPAA, OSHA, Security Risk Analysis & more!
- Practice Management Resources
  - For Everyday Issues

4

CONVENTUS

Wiks Moffat

Principal-Executive
VP of Compliance

"Compliance Consortium"

Wiks Moffat is a pioneer in the Healthcare Compliance industry and has over 25 years of experience and expertise. Currently Wiks is a Principal and Senior VP of compliance at Healthcare Compliance Network.

From 1991 to 2002 he founded and built MedSafe, Inc., working in all facets of the business. From 2002 until 2015 he worked with Total Compliance Solutions and served as president and chairman of the board.

He is a sought-after speaker to both national and state associations. He has served over 3,000 healthcare organizations in implementing regulatory compliance plans for HIPAA-HITECH, Corporate Compliance/Fraud, Waste & Abuse, billing compliance, chart auditing and OSHA safety.

What distinguishes him in the field of Healthcare compliance is his ability to make a complicated process easy to understand and to instill a culture of compliance with his clients.

5

CONVENTUS

Compliance Program Elements

6

CONVENTUS

7 Elements of a Billing Compliance Program

1. Implement Standards of Conduct
2. Compliance Officer/Compliance Committee
3. Education
4. Monitoring and Auditing
5. Reporting and Investigating
6. Enforcement and Discipline
7. Response and Prevention

7

CONVENTUS

1: Standards of Conduct/Policies and Procedures

- Promote your commitment to compliance
- Code of Conduct is meant for all:
  - Employees
  - Representatives of the organization
  - Vendors, suppliers, independent contractors
  - Board members
  - Volunteers

8

CONVENTUS

1: Code of Conduct/Policies and Procedures

- Begins with areas of risk identified within the Office of the Inspector General (OIG) Work Plan
  - Internal assessments
  - Self Disclosure
  - Regular Medicare sanction checks
  - Billing policies
  - Hotline for reporting
  - Credit balances
  - No charge visits
  - Referral sources

9

CONVENTUS

2: Compliance Officer/Compliance Committee

- "Serves as the focal point for Compliance activities"
- "Critical to the success of the program"
- Most Compliance Officers/Committees report to the CEO or the Board

10

CONVENTUS

2: Compliance Officer/Compliance Committee

- The Compliance Officer/Committee will:
  - Oversee and monitor the compliance program
  - Report to the governing body
  - Revise the compliance program periodically
  - Develop the education and training program
  - Assist with internal compliance review and monitoring
  - Independently investigate and act on matters related to compliance

11

CONVENTUS

3: Education

- The most important line of defense for a Compliance Program!
- Employees need training annually
- New hires should be trained as part of their orientation
- As new regulations change

12

CONVENTUS

3: Education

- The elements to include in a basic compliance training program:
  - Body of legal and regulatory knowledge guiding compliance activity
  - Organizations code of conduct and ethics
  - How to define and report compliance violations
  - Management needs to ensure that all employees are trained

13

CONVENTUS

3: Education

- The elements continued:
  - Only qualified personnel may perform diagnosis procedure coding
  - Physician documentation is the primary determination for claims submission
  - Vendors are held to the same compliance standards as staff
  - Employees involved in compliance violations will be disciplined.
    - Vendors will be terminated.

14

CONVENTUS

4: Monitoring and Auditing

- Ongoing evaluation is critical to a successful compliance program
- Functions common to all organizations that should be reviewed:
  - Anti-kickback and self referral issues
  - Billing and coding chart audit
  - False Claim
  - Credit balances
  - Bad debts
  - Compliance program process

15

CONVENTUS

5: Reporting and Investigating

The OIG stresses the importance of communication:

"An open line of communication between the Compliance Officer and personnel is equally important to the successful implementation of a compliance program and the reduction of any potential fraud, abuse and waste."

16

CONVENTUS

5: Reporting and Investigating

- Policy for no retaliation or retribution
  - If not, this may create whistleblowers
- Confidentiality and anonymity in the reporting process
- All complaints and investigations are monitored and tracked!

17

CONVENTUS

6: Enforcement and Discipline

- Compliance program should include a written policy setting forth the degrees of disciplinary actions that may be imposed for failure to comply with standards
- The policy should include the following 5 points:
  1. Non-compliance will result in discipline
  2. Failure to report non-compliance will result in discipline
  3. An outline of disciplinary procedures
  4. A list of the parties responsible for appropriate action
  5. A promise that discipline will be fair and consistent

18

CONVENTUS

7: Response and Prevention

- Thorough documentation of the investigation must be available
  - Description of the potential misconduct and how it was reported
  - Description of investigative process
  - List of relevant documents reviewed
  - List of employees interviewed
  - Employees interview questions and notes
  - Changes to Policies and Procedures, if appropriate
  - Documentation of disciplinary actions, if any
  - Investigations final report with recommended actions
- Voluntary disclosure

19

CONVENTUS

Enforcement is Happening: New Jersey

United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of NEW JERSEY

HOME ABOUT NEWS U.S. ATTORNEY DIVISIONS PROGRAMS

U.S. Attorneys » District of New Jersey » News

Department of Justice
U.S. Attorney's Office
District of New Jersey

FOR IMMEDIATE RELEASE Thursday, April 2, 2015

New Jersey Doctor Sentenced To Over Three Years In Prison For Taking Bribes In Test-Referrals Scheme Involving New Jersey Clinical Lab

NEWARK, N.J. – A doctor with an office in North Arlington, New Jersey, was sentenced today to 37 months in prison for accepting bribes in exchange for test referrals as part of a long-running scheme operated by Biodiagnostic Laboratory Services LLC (BLS), of Parsippany, New Jersey, its president, and numerous associates, U.S. Attorney Paul J. Fishman announced.

https://www.justice.gov/usao-nj/pr/new-jersey-doctor-sentenced-over-three-years-prison-taking-bribes-test-referrals-scheme

20

CONVENTUS

Enforcement is Happening: FBI

The Federal Bureau of Investigation

San Diego Division

U.S. Attorney's Office, Southern District of California

April 6, 2015

Mastermind of $1 Million Medicare Fraud Sentenced to 30 Months: Defendant Bilked Medicare Using El Centro Clinic

- https://www.fbi.gov/sandiego/press-releases/2015/mastermind-of-1-million-medicare-fraud-sentenced-to-30-months

21

CONVENTUS

Enforcement is Happening: OIG

- Sandoz $12.6M penalty regarding faulty drug-price reporting; March 16, 2015
  - http://oig.hhs.gov/newsroom/news-releases/2015/sandoz.asp
- $5M settlement with Medicus Laboratories LLC for alleged urine-test fraud; February 20, 2014
  - http://oig.hhs.gov/newsroom/news-releases/2014/drug-cmp.asp
- $1.5M penalty and 15-year exclusion: Joseph A. Raia, New York and New Jersey doctor accused of physical therapy fraud; March 12, 2014
  - http://oig.hhs.gov/newsroom/news-releases/2014/raia-cmp.asp

22

CONVENTUS

Security Risk Analysis (SRA)

23

CONVENTUS

According to the Department of Health and Human Services SRA

- Each Covered Entity (CE) is required to conduct an accurate and thorough analysis of the potential risk and vulnerabilities to the confidentiality, integrity and availability of ePHI.
- The CE & Business Associate (BA) must then make decisions on how to address the findings from the analysis, and manage those risks.
- The SRA should be reviewed and updated on an on-going basis.

24

CONVENTUS

HIPAA: Hackers are Here!!

- Rising Cyber Attacks Costing Health System $6 Billion Annually; Bloomberg, May 7, 2015
  - Nearly 90% of healthcare providers were hit by breaches in the past two years, half of them criminal in nature
    - http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually
- Hackers likely to breach 1 in 3 health care customers during 2016; Washington Times, December 10, 2016
  - "...healthcare data is really valuable from a cyber criminal standpoint..."
    - http://www.washingtontimes.com/news/2015/dec/10/hackers-likely-to-breach-1-in-3-health-care-custom/

25

CONVENTUS

HIPAA: Hackers are Here!!

- Cyberattack Surge: 100M medical records hacked in 2015, officials say; FoxNews.com, December 23, 2015
  - http://www.foxnews.com/politics/2015/12/23/cyberattack-surge-100m-medical-records-hacked-in-2015-officials-say.html
- "Medical records are worth up to 10 times more than credit card numbers on the black market. For a lot of [healthcare companies] it is often less of a priority than it should be. We're seeing some pretty consistent areas of non-compliance across the board."; Deven McGraw, HHS Office of Civil Rights (OCR)

26

CONVENTUS

HIPAA Audits

HHS To Launch New HIPAA Audits In Early 2016
Law 360, September 29, 2015

http://www.law360.com/articles/774290/feds-launch-long-awaited-hipaa-audits

- Random audits will include both CEs and BAs
- Will target common compliance problems
- Will include both onsite visits and remote "desk reviews" of policies
- HHS has indicated these audits will include hundreds of entities

27

CONVENTUS

HIPAA Audits

- What should you do?
  - Check your HIPAA policies and procedures!
  - Is your PHI encrypted……everywhere?
  - Are your contracts with business associates up to date?
- Regulators' top questions:
  - Did you have an incident response plan in place?
  - Did you ever practice it ahead of time?

28

CONVENTUS

Security Risk Audit (SRA)

- Identification of ePHI vulnerabilities
- I.T. Vulnerability Scan of all public facing IP addresses
- Documentation of ongoing corrective action
- Documentation of existing security elements
- Education of employees
- Communication of implemented policies including personnel sanctions
- PHI/ePHI risk management and physical security

29

CONVENTUS

HIPAA: SRA

- Chasing Down the Business Associate Agreement (BAA)
- I Need to Change my Password Again
- Create the Audit Trail
- Encryption: That Costs Too Much
- Everybody Needs to Know

30

CONVENTUS

SRA Tip sheet

Security Areas to Consider		Examples of Potential Security Measures
Physical Safeguards	• Your facility and other places where patient data is accessed • Computer equipment • Portable devices	• Building alarm systems • Locked offices • Screens shielded from secondary viewers
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement
Technical Safeguards	• Controls on access to EHR • Use of audit logs to monitor users and other EHR activities • Measures that keep electronic patient data from improper changes • Secure, authorized electronic exchanges of patient information	• Secure passwords • Backing-up data • Virus checks • Data encryption
Policies & Procedures	• Written policies and procedures to assure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Business associate agreements	• Plan for identifying and managing vendors who access, create or store PHI • Agreement review and updates

https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

31

CONVENTUS

Chasing Down the BAA

Secure the BAAs

- CEs are required to secure BAAs with BAs
- BAs are now required to secure BAAs with its subcontractors

32

CONVENTUS

Why BAA's

- BAAs protect the CE
- BAAs make protecting PHI/ePHI a shared responsibility
- BAAs are a BA's written promise to protect PHI/ePHI in accordance with federal laws
- Without BAAs, the CE is essentially sharing PHI with no written promise to protect it and with no shared liability
- BAAs are required!

33

CONVENTUS

Who are my Organization's BA's?

Examples:

- Software Vendor with ePHI/PHI Access
- Shredding Service
- IT Service Provider
- Answering Service-Appointment making service
- Billing Service or Clearinghouse
- Collection Agency
- Transcriptionists
- Record Archival Service
- Appointment Reminder Service

34

CONVENTUS

Time for Introspection

35

CONVENTUS

2016 Office for Civil Rights (OCR) Audits

- The OCR will look into security, privacy and breach notification rules to analyze risk, safeguards and implementations
  - Especially those associated with electronic health information and device encryption

36

CONVENTUS

HIPAA Introspection

A few things to ask yourself:

- Do we have written policies and procedures?
- Are we performing and documenting regular risk assessments?
- Do we have an incident response plan?
- Mobile devices and storage media?
- Are our business associates audited?
- Training program informs new staff members and periodically refreshes existing workers on HIPAA compliance?

37

CONVENTUS

Response and Prevention

- Violations of compliance programs threaten an organizations status
- Failure to respond, or to engage in lengthy delay can have serious consequences
- If a problem is found the first step is to meet with your legal counsel to determine the severity and develop a plan of action
- OIG requires prompt reporting to the appropriate authority within a reasonable time, but not more that 60 days

38

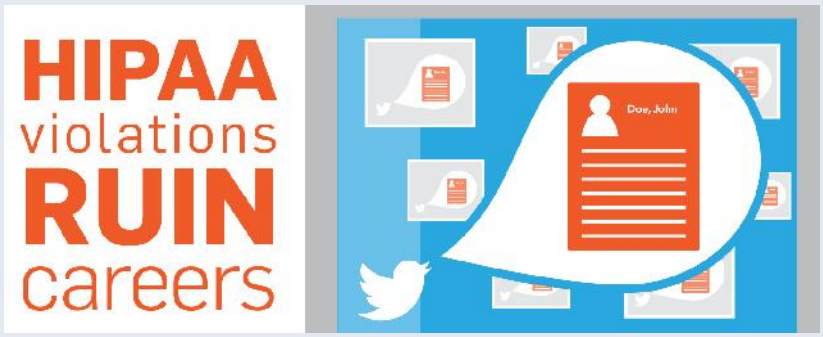
CONVENTUS

HIPAA Enforcement

- HIPAA Privacy, Security, and Breach Notification Audit Program
- As a part of our continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the HHS OCR has begun its next phase of audits of CEs and their BAs
  - The 2016 Phase 2 HIPAA Audit Program will review the policies and procedures adopted and employed by CEs and their BAs to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules

39

CONVENTUS



HIPAA Violations

- Up to $50,000 per violation with a maximum of $1,500,000 per year
- Individual can be help criminally liable

40

CONVENTUS

HIPAA: Wall Of Shame

- Breaches Affecting 500 or More Individuals
  - Providers who have reported breaches of unsecured PHI are required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals.
  - These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice PHI to the Secretary. The following breaches have been reported to the Secretary
  - Potential $1,500,000 fine. Not to mention reputational damage.

41

CONVENTUS

Compliance Program

The OIG has stated the following:

"The best evidence that a provider's compliance program is operating effectively occurs when the provider, through its compliance program identifies problematic conduct, takes appropriate steps to remedy the conduct and prevents it from recurring, and makes a full and timely disclosure of the misconduct to the appropriate authority."

42

CONVENTUS

How to get Stakeholders and Doctors to Buy Into a Culture of Compliance?

- Give them the cold hard facts
- Condition of Participation
- Offer to take charge and do it for/with them
- Budget
- Plan
- Be proactive and protective…not reactive

43

CONVENTUS

Questions

Resources

- www.hcca.com
- Compliance101 Third Edition

44

CONVENTUS

Speaker Contact Information

Wiks Moffat, CHC

Principal-Executive VP of Compliance

Healthcare Compliance Network/
Compliance Consortium, LLC

617-803-3352

wmoffat@hcompliance.com

www.hcompliance.com

HCN HEALTHCARE COMPLIANCE NETWORK, INC.

45

CONVENTUS

Conventus Contact Information

Susan Lieberman, MBA, BSN

Vice President, Conventus Practice Resources

Conventus Inter-Insurance Exchange

Phone: 877-444-0484, x.7466

susanlieberman@conventusnj.com

www.conventusnj.com

46

CONVENTUS

47