Behavioral Healthcare Compliance: It's Time to Take it Up a Notch

Terese Farhat
TFarhat@ClarkHill.com

Objectives:

1. Increase awareness of healthcare reform (Affordable Care Act) and its impact on behavioral health providers

2. Discuss how health reform measures have affected government investigation and enforcement actions against providers

3. Identify areas of risk to behavioral health providers based on recent government activity (both state and federal)

4. Describe methods and opportunities to assist providers develop and/or improve the effectiveness of compliance activities

Notes:
Behavioral Healthcare Compliance: It's Time To Take It Up A Notch

Terese Farhat
Clark Hill PLC
151 S. Old Woodward Ave.
Suite 200
Birmingham, MI  48009
248-988-5878

Alphabet Soup

- CMS – Centers for Medicare/Medicaid Services
- HHS – Health and Human Services
- DOJ – Department of Justice
- OIG – Office of Inspector General
- OCR – Office of Civil Rights
- ACA – Patient Protection and Affordable Care Act
- HIPAA – Health Insurance Portability and Accountability Act
- HITECH Act – Health Information Technology for Economic and Clinical Health
- PHI – Protected Health Information
- ePHI – Electronic PHI
- IDD – Intellectual and Developmental Disabilities
- PCS – Personal Care Services
- FMV – Fair Market Value
- BA – Business Associate

The New War Against Healthcare Fraud

- Health Care Fraud Prevention & Enforcement Action Team (HEAT)
- 2009 joint initiative between DOJ and HHS
- HEAT has expanded from 2 to 9 locations throughout the U.S. – there is now one in Detroit
- Dedicated joint efforts to prevent fraud and enforce anti-fraud laws
- Ongoing efforts to identify new enforcement initiatives and areas for increased oversight
- Medicare Fraud Strike Force teams are a key component of HEAT
The New War Against Healthcare Fraud

- May 2, 2012 - Nationwide Medicare Fraud Strike Force takedown
- 187 individuals charged - charges totaled $452 million in alleged false billings
- Highest amount of false billings in a single takedown in strike force history
- 22 Detroit area residents charged
- Focus was on mental health service providers, psychotherapy services and adult day care centers - providing services not medically necessary or not provided at all
- Detroit identified as the “new frontier” for healthcare fraud
- Disturbing trend noted – exploitation of elderly or compromised adults
- Providers of those individuals are being targeted
- Detroit AUSA McQuade quoted as saying, “we want providers to know that we are scrutinizing billing records….we are seeking very strong sentences…”

The War Continues....

- October 4, 2012
- Strike Force operations in 7 cities led to charges against 91 individuals and $430 million in false billings
- Indictments charged more than $100 million in mental health care fraud
- Claims include billing for services that were medically unnecessary, never provided, or not documented properly

STATS for 2012

- Fiscal year 2012 - $4.2 BILLION ($4.1 Billion for 2011)
- ROI highest 3-year average ($7.95 recovered for every $1 spent)
- 1,131 new criminal health care fraud investigations were opened involving 2,148 defendants
- 826 were convicted of health care related crimes (average prison sentence was more than 48 months)
- 885 new civil investigations opened
- 400,000 providers were subject to new screening requirements
- 150,000 lost the ability to bill Medicare program due to ACA’s new requirements and initiatives
- 3,131 individuals and entities excluded by OIG
  - 212 were due to patient abuse or neglect
  - 912 were related to crimes related to Medicaid and Medicare
Patient Protection and Affordable Care Act (ACA)

- Provided new tools to strengthen anti-fraud efforts
- $350 million over the next 10 years
- Investments in sophisticated data analytics and more “feet on the street” law enforcement agents
- Contractors (paid on contingent fee basis) have been expanded to Medicaid arena
- Tougher sentencing and increased financial penalties by 20-50%
- New focus on compliance by detection and prevention – as opposed to “pay and chase”

MANDATORY EFFECTIVE COMPLIANCE PROGRAMS

ACA section 6401 applies to all providers and suppliers that participate in Medicaid and Medicare – as a condition of enrollment

WHAT DOES THIS MEAN?

- Government is looking at all types of providers
- Using fraud detection computer programs and other data analytics to find abnormalities in Medicaid/Medicare claims
- Entities that provide services to the most vulnerable are targeted – mental health and IDD providers are at risk
- It’s not just about the “really bad actors” anymore
- Focus is on quality of care, billing for medically unnecessary services or billing for services that were not provided or not documented
- No longer just focusing on cities like Miami, FL

YOU NEED TO PAY ATTENTION TO COMPLIANCE

Fraud by Behavioral Health Providers

- Settlement reported on May 1, 2012
- Psychiatric Solutions Inc. and Universal Health Services Inc.
- Joint agreement to pay $3.45 million to settle fraud allegations involving provision of mental health services
- Government claimed the facility failed to meet conditions required for payment
  - Failure to obtain approval of certain outpatient treatment
  - Failure to document individual outpatient therapy sessions
  - Failure to obtain physician orders for certain lab work
  - Failure to obtain physician certifications for admissions
- Whistleblower in the case received $587,000
Local Mental Health Provider Closes Doors After Allegations of Medicaid Fraud

Story hit Idaho's KPVI News 6 on April 3, 2013

East Idaho provider of mental health services

Credible allegations of fraud against the provider and ongoing investigation

Idaho Department of Health and Welfare took following actions:

- suspended all Medicaid payments
- sought recoupment of overpayments - $439,659.11
- imposed CMPs (civil monetary penalties) in the amount of $109,941.79; and
- immediately terminated provider agreements for a period of 5 years.

Idaho Provider Case

Credible allegation of fraud is defined as an intentional deception or misrepresentation made by person with knowledge that the deception could result in some unauthorized benefit to himself or some other person.

Department reviewed mental health clinic, psychosocial rehabilitative and developmental services billed by provider and found issues such as:

- billing for services not documented
- billing for services with overlapping times
- non-covered services billed as covered services
- billing for medically unnecessary services
- billing for services exceeding service limitations

Findings of Deficiencies

- Non-covered billed as covered
  - services billed without valid treatment plans (e.g. missing required signatures)
  - clinic services were billed with no initial evaluation or CDA (comprehensive diagnostic assessment)
- Medically unnecessary services
  - diagnoses not supported by records
  - services billed without completing CDAs
  - services billed were not listed on treatment plan
Findings of Deficiencies (Con’t)

- Documentation Issues
  - no documentation found for services billed
  - cloned progress notes (using same notes to document multiple services for the same or multiple clients)
  - provider documented providing services to more than one client during same period of time
  - overbilled units of service (billing should have been for 1 unit based on duration of session instead of billing multiple units)
  - backdated records
  - supervising physician admitted to signing treatment plans and back-dating them
- Conflicting documentation

OIG 2013 WORK PLAN

Areas of focus and increased scrutiny:
- Medicaid Waivers – Quality of Care
- Home, Community, Personal Care and School-Based
  - focus on plans of care, whether services were received as stated in their plans, and whether services were provided by qualified providers
- Home and Community Based Services – Adult Day Care
  - necessity, eligibility, and furnishing of services in accordance with plan of care
- Transportation Services
  - review of necessity and beneficiary eligibility

"Medicaid personal care programs are targets for fraud, investigators say"

- Report by OIG (6 years worth of investigations)
- Fault placed with CMS for inadequate oversight of the programs and CMS has been asked to "step up to the plate"
- "Lucrative target for fraud" due to:
  - lax requirements for both caregivers and patients in combination with poor state and federal oversight
  - poor claims documentation
  - insufficient monitoring of claims data for fraud, waste and abuse
  - various qualifications/requirements for care workers in different states
- 2011 Medicaid paid more than $12 BILLION for PCS (up 35% since 2005)
- 2010 Medicaid Fraud Units investigated more than 1,000 cases involving PCS – more than any other type of Medicaid service
OIG – AUDIT OF LOUISIANA MEDICAID PCS

- January 2013 Report of a Louisiana provider
- 100 claims in random sample; 72 did NOT comply
  - services were provided by employees who did not meet minimum training
    requirements or did not meet minimum education and experience
    requirements
  - provider did not have sufficient documentation to support number of units
    billed
- State did not effectively monitor its PCS providers for compliance
- Refund of $820,096 for unallowable PCS
- Recommendations
  - ensure PCS providers implement controls to ensure their employees meet
    all applicable training requirements
  - ensure PCS providers understand employee training requirements and that
    provider improves its monitoring of PCS to identify issues of non-compliance

OIG – AUDIT OF NEW MEXICO MEDICAID PCS

- State paid provider $405,000 for PCS claims that did not
  comply with federal and state requirements
- 100 claims in random sample; 24 did not comply
  - inadequate attendant certifications (i.e. TB testing, CPR)
  - no documentation of supervisory visits
  - unsupported units of service claimed
  - no documentation of physician authorization
- Refund of $404,817 for unallowable services

OIG – AUDIT OF MISSOURI MEDICAID PCS

- March 2013 Report of Missouri provider
- Findings included:
  - Assessment or reassessment was not performed within
    required time frames
  - Plans of care were either missing or not approved
  - Documentation incomplete – requirement that beneficiary be
    trained as specified in the State regulations
- Refund of $143,397 to Feds
- Requirement to improve policies and procedures for
  monitoring PCS program for compliance with state and federal
  requirements
Compliance Program

- Standards, Policies and Procedures
  - Do you have a Code of Conduct?
  - Do you have comprehensive, understandable policies?
  - Do they exist for all relevant topics such as HIPAA and reporting of breaches, IT security, non-retaliation, annual training requirements, orientation, reporting, coding and billing standards, documentation standards, conflicts of interest?
  - Has a risk assessment been done recently?

- Oversight
  - Do you have a dedicated Compliance Officer with high level of authority who reports to the CEO/Director or the Board?

Compliance Program

- Ongoing Training and Education
  - Do you have compliance training for all new hires?
  - Do you have mandatory annual compliance training?
  - How do you communicate compliance related information with your workforce? Do you use email blasts, newsletters, staff meetings to discuss compliance related topics?
  - Do you provide specialized updates or information like changes with Medicare or Medicaid requirements, supervision requirements, documentation required to support certain coding?
  - Do you measure compliance knowledge after training/education?
  - Do you document staff training/education was provided?

Compliance Program

- Open lines of communication for reporting
  - Do you have a dedicated mechanism(s) for employees to report concerns?
  - Is there a telephone “hotline” available for staff to report anonymously and confidentially?
  - How do you track and respond to calls or reports made?
  - Are the methods well-publicized and known at all levels? Do staff know what to report?

- Ongoing monitoring and auditing
  - Do you monitor coding and billing routinely? What is the quantity, method and frequency?
  - What internal controls do you have in place to ensure documentation meets the coding used and level of reimbursement received?
  - How do you manage your financial and compensation arrangements with providers, vendors, suppliers? Are you receiving free or discounted items or services? What about paying more or less than FMV for items or services?
  - How are the risk areas identified?
  - What do you do with audit results?
  - How do you handle billing errors if and when identified? Is there a process in place?
  - Do you use external auditors – independent with no vested interest?
AUDIT PLAN – RISK AREAS OF FOCUS

- INDIVIDUAL PLAN OF SERVICE (IPOS), PLAN OR TREATMENT PLAN
- DOCUMENTATION OF SERVICES
- CASE MANAGEMENT FUNCTION
- STAFF SCREENING
  - LICENSURE, CREDENTIALS, QUALIFICATIONS, SCOPE OF PRACTICE
  - EXCLUDED PROVIDERS
  - CRIMINAL BACKGROUND CHECKS

IPOS

- Person-centered planning process
- Identifies the needs and goals of the consumer/recipient
- Must identify the need for services (e.g. support medical necessity):
  - clinically appropriate
  - necessary to meet the needs
  - consistent with person's diagnosis, symptoms and functional impairments
  - most cost-effective option in the least restrictive environment
  - consistent with standards of care
- Sets forth the scope, amount, and duration of services
- Authorizes the services and supports to be provided
  - MUST BE DOCUMENTED AND SIGNED

DOCUMENTATION

- Generally, services are covered only when authorized by a physician or health care professional in accordance with IPOS
- Provider of service must meet the required qualifications
- Documentation must sufficiently reflect the services provided and support claims for payment
- The following documentation must exist:
  - assessment of beneficiary's needs that supports services requested
    - plan should include the specific supports, services and activities, including amount, scope and duration to be delivered that is approved at least annually during person-centered planning
    - documentation of the specific days, time (if unit based) and description of services provided consistent with the IPOS/plan of care
CASE MANAGER
- CORE OF RISK
  - Covered service that assists individuals to design and implement strategies for obtaining services and supports
  - Must assure person-centered planning process and that it results in an IPOS
  - Identifies services and supports that will be provided, who will provide them, and how the case manager will monitor (i.e. interval of face to face contacts) the services/supports identified under each goal and objective
  - Oversight over implementation of IPOS
  - Identify and address gaps
  - Coordination of services and supports, assist with access, facilitate transitions, assist with crisis planning and after-hours contact
  - RECORD MUST CONTAIN SUFFICIENT DOCUMENTATION TO VALIDATE THIS SERVICE

IF IT WASN’T DOCUMENTED, THEN IT WASN’T DONE…..

IF IT WASN’T DONE AND CLAIM OR ENCOUNTER WAS SUBMITTED FOR REIMBURSEMENT…
THEN THERE MAY BE A BASIS FOR A FALSE CLAIM ALLEGATION
CREDENTIALS AND QUALIFICATIONS
- Reimbursement is not allowed for services and supports provided unless the provider meets the Medicaid/Medicare requirements for provider qualifications
- Training requirements must be met and documented
- Must validate and document background, qualifications, licensure if applicable, registration and credentials – recommend PRIMARY SOURCE VERIFICATION
- Pay attention to scope of practice

OIG EXCLUSION AUTHORITY
- OIG has the ability to exclude individuals and entities from participating in the federally funded health programs – Medicaid and Medicare
- Exclusion of a person affects the ability of the organization to claim payment for items/services
- No payment shall be made for items/services furnished, ordered or prescribed by an excluded individual or entity (all methods of reimbursement)
- Applies to excluded person and anyone who employs or contracts with the excluded person – even applies to administrative and management services furnished by excluded person

SCREENING REQUIREMENTS
- You must screen all employees and contractors to determine whether any of them have been excluded from federal health programs
- Use HHS' OIG Web site to search the List of Excluded Individuals and Entities (LEIE)
- Recommend search performed monthly and maintenance of documentation that you completed the searches
- Don’t forget about State law requirements – criminal background checks
Compliance Program

- Enforcement & Discipline
  - Is there real accountability?
  - What is the process for disciplinary action? Is the process incorporated in your HR practices?
  - Consistently in application?
  - Policy of non-retaliation?

- Response & Prevention
  - Do you have a complaint response procedure?
  - Do you perform regular and routine screening (LEIE) excluded provider checks? Are you documenting these?
  - Do you have a process and procedure when overpayments are identified?
  - How robust is your QA program?

HIPAA and HITECH

- HIPAA – Enacted in 1996 to protect the privacy and security of certain health information
  - Privacy Rule – Sets national standards for the protection of health information
  - Security Rule – Specifically applies to electronic protected health information

- HITECH Act – Enacted in 2009 to strengthen HIPAA enforcement and penalties and instituted breach notification requirements

- HHS’ Office of Civil Rights (OCR) enforces these Rules

HIPAA Privacy Rule - Summary

- Limits the uses and disclosures of patient information
- Creates individual rights to inspect, copy, amend, request restrictions, file complaints and receive notice of privacy practices
- Requires agreements with business associates to safeguard information
- Requires privacy policies and procedures (P/P)
- Designation of a Privacy Officer and contact person to receive complaints
- Requires implementation of safeguards to protect PHI
- Requires training of all employees
- Sanctions against workforce members who fail to comply with P/P
- Precludes retaliation against those who report or file complaint
HIPAA Security Rule - Summary

- Covered entities must:
  - Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by their workforce.

FINAL HIPAA RULE

- OCR released Final Rule on January 17, 2013
- Final Rule takes effect March 26, 2013
- Enforcement begins on September 23, 2013
- Highlights:
  - Business Associate (BA) definition is broadened (e.g., includes BA’s subcontractors)
  - BA’s will have direct liability for compliance under certain HIPAA Privacy Rule and Security Rule provisions
  - Definition of marketing is expanded and requires authorization from patient
  - Sale of PHI requires express written authorization
  - Fundraising communications require providing individuals opportunity to “opt out” of receiving further fundraising materials

HIGHLIGHTS OF HIPAA FINAL RULE (CON’T)

- Breach notification substantially changed
  - OCR abandoned “significant risk of harm” standard in favor of a more objective test
  - Presumption of breach in all cases of breach involving unsecured PHI unless documented risk assessment demonstrates low probability that PHI has been compromised (involves 4-factor risk assessment)
- Notice of Privacy Practices
  - Authorization requirement for most uses and disclosures of psychotherapy notes (if applicable), PHI for marketing purposes, sale of PHI
  - If PHI used for fundraising, the individual must be notified that he/she has right to opt out of receiving such communications
  - Individual has right to be notified in the event of a breach of unsecured PHI
HIGHLIGHTS OF HIPAA FINAL RULE (CON’T)

- **Access to ePHI**
  - right to access and copy PHI within 30 days of request
  - right to receive electronic copies of PHI that is maintained electronically in one or more designated record sets
  - must honor electronic form and format requested by the individual if PHI is readily producible or, if not, in a readable electronic form and format as agreed to by the entity and individual

- **Enforcement**
  - incorporates 4 categories of violation based on level of negligence [e.g. did not know, reasonable cause, willful neglect (corrected) and willful neglect (not corrected)]
  - $1.5 million cap for all violations of identical provision in a calendar year (liability may exist for multiple violations of multiple provisions and will be counted separately)

---

**Required Actions**

- Modify Notice of Privacy Practices and Authorization Forms
- Update and/or execute new business associate agreements
- Revise HIPAA policies and procedures, including breach notification procedures

---

**Impermissible Uses and Disclosures**

- **General Rule** – covered entity may not use or disclose PHI unless
  - a patient (legal representative) authorizes it in writing; or
  - it is permitted or required by the Privacy Rule
- **Permitted Uses/Disclosures** means that you are “permitted” to use or disclose PHI without the need for patient authorization
- **Examples of permitted uses/disclosures** include:
  - treatment, payment or health care operations
  - required by law (i.e. Patient and Advocacy system)
  - public health activities (i.e. reporting abuse or neglect)
  - law enforcement (only if certain conditions are met)
Uses and Disclosures: Psychotherapy Notes

- To disclose psychotherapy notes, a covered entity must obtain a written authorization, unless the disclosure is:
  - to carry out the following treatment, payment or healthcare operations
  - used by the originator of the psychotherapy note for treatment
  - used by the covered entity to defend itself in a legal action or other proceeding brought by the individual
  - HHS investigation to determine compliance with Privacy Rules
  - to avert serious and imminent threat to public health or safety
  - to a coroner or medical examiner
  - required by law

Access

A covered entity is required to disclose PHI if:
- an individual requests his/her own PHI – access to PHI or an accounting of disclosures of their PHI; or
- when requested by HHS for a compliance investigation/review or enforcement action.

Minimum Necessary

- Must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request
- Reasonable efforts means covered entities should evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information.
Minimum Necessary: Exceptions

- Disclosures or requests by a healthcare provider for treatment
- Uses or disclosures made to the individual
- Uses or disclosures made pursuant to a valid authorization
- Disclosures made to the Secretary of HHS
- Uses or disclosures required by law
- Uses or disclosures required for complying with HIPAA

Notice of Privacy Practices (NPP)

- Individuals have a right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity and the individual’s rights and the covered entity’s legal duties with respect to the PHI
- Direct treatment providers – provide NPP on date of 1st service delivery and written acknowledgement of receipt of NPP or good faith effort to obtain the acknowledgement
- Must be available upon request to any person
- If you have a website, the notice must be prominently posted
- Must document compliance with this requirement by retaining copies of the notices issued by the covered entity

HIPAA Security Rule

- Risk analysis required – 1st step
- Flexible approach - covered entities may adopt/use any security measures that allows for reasonable and appropriate implementation of the standards and specifications of the Rule
- Covered entities must take into account the following factors in deciding which security measures to use:
  - The size, complexity and capabilities of the covered entity;
  - The covered entity’s technical infrastructure, hardware and software security capabilities;
  - The costs of security measures; and
  - The probability and criticality of potential risks to ePHI.
Security Rule

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Administrative Safeguards

- Administrative safeguards require covered entities to perform risk analysis as part of their security management processes:
  - Evaluate the likelihood and impact of potential risks to ePHI;
  - Implement appropriate security measures to address the risks identified in the risk analysis;
  - Document the chosen security measures and, where required, the rationale for adopting those measures; and
  - Maintain continuous, reasonable and appropriate security protections.
- The risk analysis should be ongoing – it’s not a one-time occurrence

Administrative Safeguards

- Security Officer – Designate a security official who is responsible for the development and implementation of the Security Rule
- Information Access Management – Implement policies and procedures for authorizing access to ePHI only when the access is appropriate based on the user or recipient’s role
- Workforce Training – A covered entity must provide for appropriate authorization and supervision of its workforce, must train its workforce on its security policies and procedures and have sanctions against those who violate the policies and procedures
- Evaluation – Periodic evaluation of the policies
Physical Safeguards

- Facility Access and Control – Covered entities must implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

- Device and Media Controls – Covered entities must implement policies and procedures governing the receipt, transfer, removal, disposal and re-use of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility.

Technical Safeguards

- Access Control – Implement technical policies and procedures to allow access only to those persons or software programs that have been granted access rights to ePHI
  - Unique user identification – Assigning a unique name/number for identifying and tracking users
  - Emergency access procedures – Implementing procedures for accessing ePHI during emergencies
  - Automatic logout – Terminating a session after a certain amount of time of inactivity
  - Encryption and decryption – Implementing mechanisms to encrypt and decrypt ePHI
Technical Safeguards

- Audit Controls – Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI
- Integrity Controls – Implement policies and procedures to protect ePHI from improper alteration or destruction
- Person or Entity Authentication – Implement procedures to verify that a person or entity seeking access to the ePHI is the one claimed
- Transmission Security – Implement measures to guard against unauthorized access to ePHI transmitted electronically

HIPAA Enforcement Actions

- University of California at Los Angeles Health Systems (July 2011)
  - Repeated access to patient records by employees without permission and not in connection with treatment reasons
  - Failure to implement policies and procedures to demonstrate compliance with Privacy and Security Rules
  - 3-year corrective action plan and $865,000 settlement amount
- Blue Cross Blue Shield of Tennessee (March 2012)
  - Computer servers on which ePHI of 1 million individuals was stolen from a facility
  - Found failures to have appropriate administrative and physical safeguards
  - 18 corrective action plan and $1.5 million settlement amount

HIPAA Enforcement

- June 28, 2012 – the Alaska Department of Health and Social Services (“Alaska Medicaid”) agreed to pay $1.7 million to settle possible violations of the HIPAA Security Rule – allegations include a stolen USB hard drive possibly containing ePHI stolen from the vehicle of a DHS employee.
  - The OCR’s investigation revealed the following:
    - Alaska Medicaid did not have adequate policies and procedures in place to safeguard ePHI
    - Alaska Medicaid did not:
      - complete a risk analysis
      - implement sufficient risk management measures
      - complete security training for its employees
      - implement device and media controls
      - address device and media encryption
Violations Do Not Require Knowledge of HIPAA

- United States v. Zhou, No. 10-50231 (9th Cir. May 10, 2012)
- Following termination from UCLA Health System of his termination, Dr. Zhou accessed patient records without authorization – mostly from co-workers and celebrities
- He argued that he did not knowingly violate HIPAA
- Court held that Dr. Zhou did not have to know that it was illegal to access the records
- What is the take away?
  - statute does not require “knowledge” that actions are illegal under HIPAA
  - “knowledge” applies only to the act of obtaining the health information

Heightened Enforcement

January 2, 2013 – HHS announced first settlement in smaller data breach

- Hospice of North Idaho settled alleged violations with OCR for $50,000
- First settlement stemming from a HIPAA Security Rule violation for breach affecting LESS than 500 individuals
- Hospice used laptops in the field, but:
  - did not have policies/procedures to address mobile device security
  - had not conducted a HIPAA-mandated risk analysis to safeguard e-PHI
- Regardless of size, covered entities must take action and will be held accountable for safeguarding PHI

WHAT SHOULD YOU BE ASKING?

- Are we getting complete treatment plans? Do they need to be revised to address progress or changed needs?
- What is currently being documented and does it support codes used for the services provided? Do documentation of services support the plans?
- Do we have sufficient staffing to ensure that the required level of service is being delivered?
- Are the providers properly trained and qualified for the type of service provided?
- Do you have documentation to support training and qualifications for each staff member?
MORE OF WHAT YOU SHOULD BE ASKING...

- Are staff spread too thinly to adequately perform job – quality concerns?
- Do the providers actually know and understand what is expected in terms of documentation requirements?
- Is the right person performing the monitoring/auditing function?
- Is there documentation to support the routine monitoring and audits performed?
- What is done when an error or overpayment is identified?

NOW WHAT?

- IT’S TIME TO TAKE IT UP A NOTCH
- If you have a compliance program – it’s time for a “facelift”
- If you don’t have one – it’s time to begin developing one
- Consider a risk assessment of your organization to put it in the best shape from a compliance standpoint
- Threats are very real
- YOU CAN NO LONGER AFFORD TO IGNORE, KEEP YOUR HEAD IN THE SAND AND HOPE FOR THE BEST

WE CAN HELP YOU

- Clark Hill offers a number of services that can help you – creative and customized both in scope and cost to fit your needs and resources
  - Perform a risk assessment of your current program
  - Draft Code of Conduct and Policies/Procedures or review existing P/P
  - Provide education and training for staff
  - Board/Governance counseling/guidance
- Benefits to you
  - Qualified legal experts
  - Attorney client privilege protections
  - Independent assessment by unbiased reviewer – objectivity
  - Alternative fee structuring depending on the size of your organization and services needed