• No comments received on RP2 Annual Report
• Repaid extrapolation from Claims Review
  – RP3 Claims Review facility list and selection will occur in Spring 2019
Elements of the MU Health Compliance Program

Organized in accordance with the seven elements outlined by the DHHS OIG for effective compliance programs

1. Designate a compliance officer and compliance committees
2. Develop written compliance plans, policies, and standards of conduct
3. Monitor and audit compliance risk areas
4. Develop open lines of communication
5. Implement education and training
6. Enforce disciplinary standards
7. Respond to detected deficiencies
Visualizing Effective Compliance

Compliance Officer & Committee

- Enforce Standards
- Respond to Deficiencies

- Written Policies & Procedures
- Open Communication
- Training & Education
- Monitoring & Auditing

OPEN – HEALTH AFF – INFO 2 – 4
Operationalizing Effective Compliance

- Lead & Organize
- Address Concerns
- Innovate & Improve
- Set Expectations
- Share Lessons Learned
- Train & Educate
- Review & Assess
• Work Plan Status
  – ~5 “ad hoc” requests/month
    • not included in work plan figures

• Current Efforts
  – Supporting Pharmacy 340B HRSA Audit
  – Analyzing Coding & Billing Quality Data from UP Accuracy Vendor
  – Regulatory Change Management
  – Revising all OCC publications
  – Policy Development Projects
    • Ex: Chaperones; Therapy Animals; Visitors

COMPLIANCE PROGRAM UPDATE

- Completed: 25%
- In Flight: 41%
- Recurring Audits: 8
- New Additions: 9

OPEN – HEALTH AFF – INFO 2 – 6
• Sean Rivera, MU Health Information Security Officer

• Information Security is:
  – Processes and methodologies designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption
  – In short, preserve the **Confidentiality, Integrity, and Availability** of data
INFORMATION SECURITY PROGRAM UPDATE

NEWS

Third-party vendor error exposes data of 19K patients for 2 months
by Jessica Davis | August 02, 2018

Orlando Orthopaedic’s transcriptionist vendor misconfigured access to a database during a software upgrade. The health center waited

NEWS

Nearly 280,000 Medicaid patient records breached in Oklahoma hack
by Jessica Davis | January 15, 2018

A hacker gained access to an Oklahoma State Health Sciences network and accessed folders containing Medicaid billing data.
Why is Healthcare Data So Valuable?

Financial data has a finite lifespan because it becomes worthless the second the customer detects the fraud and cancels the card or account. Most forums for such data have a high enough surplus of stolen payment cards that they have fire sales.

But information contained in health care records has a much longer shelf life and is rich enough for identity theft. Social Security numbers can't easily be cancelled, and medical and prescription records are permanent. There's also a large market for health insurance fraud and abuse, which may be more lucrative than simply selling the records outright in forums.
Program Accomplishments to date:
• Revised Information Security Program Policy
• Established Information Security Advisory Council
• Adopted Critical Security Controls
• High-Level risk assessment
• Increased cyber security posture with tools in place
• Started education and awareness efforts
• Daily Activities include:
  – policy and procedure ownership
  – procurement reviews
  – incident tracking
Office of Corporate Compliance Staffing Updates

Retired: Tina Adams-Salter, System Privacy Officer

System Privacy Officer provides oversight and direction of the MU Health privacy program; HIPAA rules compliance and enforcement; Privacy education and training; Assess privacy risks and coordinate organization-wide protections for our patients' protected health information

Recruitment in process