OFFICE OF AUDIT, COMPLIANCE AND PRIVACY
FY2017

Greg Pellicano
Associate Vice President
Audit, Compliance and Privacy
(1)

Pat O’Toole
Administrative Support
(1)

Frank Tresnan
Executive Director
Internal Audit
(1)

Judy Bolch
LGH Director Internal Audit
(1)

Scott Schafer
University Privacy Officer
(1)

Linda Yoder
Institutional Compliance Officer
(1)

Lauren Steinfeld
Institutional Chief Privacy Officer and Senior Advisor for Privacy
(1)

Chad Borden
University Assistant Privacy Officer
(1)

Alena Abrosimova
University Audit Manager
(1)

Joyce Massott-Burnett
Penn Medicine Audit Manager
(1)

Kevin Secrest
IT Audit Manager
(1)

Amanda Smith
Supervisor Financial Audits
(1)

John Dunn
Jeoff Young
Vacant
Information Systems Auditor
(1)

Sarah Finnerty
Privacy Analyst
(1)

Stephen Holroyd
Mary Seng
University Sr. Internal Auditor
(2)

Tracey Caputo
Anna Grochocinska
Jennifer Sholder
Erin Thornton
Vacant
Penn Medicine Sr. Internal Auditor
(5)

Dan Hill
Dom Pasquaino
Sr. IT Audit Specialists
(2)

Joseph Bentz
Shawn Strauss
Senior Sr. Financial Auditor
(2)

Compliance Co-Op Intern

Ben Geevarghese
IT Auditor
(1)

Vacant
Internal Auditor
(1)

Mary Seng
Sr. Internal Auditor
(2)

Sarah Finnerty
Privacy Analyst
(1)

Greg Wilson
Internal Auditor
(1)

Vacant
Internal Auditor
(1)

Amanda Smith
Supervisor Financial Audits
(1)

John Dunn
Vacant
Information Systems Auditor
(1)

Joseph Bentz
Shawn Strauss
Senior Sr. Financial Auditor
(2)

Vacant
Internal Auditor
(1)

30 Headcount
(9.5 Univ, 13.5 Penn Med, 7 LGH)

= University
= Penn Medicine
= Lancaster General Health
= Shared University and Penn Med
INTERNAL AUDIT

Internal audit is:
• an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.

Internal control is:
• a process effected by an organization to provide reasonable assurance that organizational objectives will be met in the following categories:
  • Effectiveness and efficiency of operations
  • Reliability of financial reporting
  • Compliance w/ applicable laws & regulations
  • Safeguarding of assets
INSTITUTIONAL COMPLIANCE

- Provides resources to help University and Penn Medicine faculty, staff and students maintain the highest ethical standards and abide by all legal requirements, policies, and procedures

- 215-P-Comply Line
- Principles of Responsible Conduct
- University Policies
- Liaison Network
- Clery Act Reporting – Annual Security & Fire Safety Report
UNIVERSITY PRIVACY

• Provides resources on a wide range of privacy issues affecting the members of Penn’s community

• **Privacy & Security Training**

• **Protecting Penn Data**
  • Security and Privacy Impact Assessment (SPIA) Program
  • Strong Security Protections
  • Evaluating Third Parties
    • SPIA For Vendors
  • Reporting Incidents

• **Protecting Your Own Data**

• **Policies & Guidance**
Supports the development and deployment of policies, procedures, and processes to safeguard patient privacy and the privacy and security of patient information.

- HIPAA Focused
- Business Associate Agreements
- Patient Privacy Policies/Options
- Incident Response
- Accessing and Sharing Electronic Protected Health Information
SCHOOL AND CENTER AUDIT COMMON ISSUES

• Lack of Financial Oversight and Monitoring
• Non-compliance w/ Purchasing Card Guidelines
• Duties Not Segregated
• Inadequate Cash Controls
• Improper Worker Classification/Policy Compliance
• Unsupported/Inadequately Supported Cost Transfers
• Lack of PI Approval of Sponsored Project Expenditures
PENN MEDICINE AUDIT COMMON THEMES

- Revenue Cycle
  - Ineffective Charge Capture Process
  - Segregation of Duties – Write-offs/Credits
- Human Subject Payments
- IRB Compliance
- Research versus Standard of Care (Insurance) Billing
INFORMATION TECHNOLOGY AUDIT COMMON ISSUES

- Cyber Security/Data Security Exposures
- Vendor Management/IT Contracting
- Inadequate IT Physical Security
- Insufficient Web Application Security
- Excessive Administrative Rights
- Inappropriate Access
- No Review of System Logs
- Failure to Secure Sensitive Data
COMPLIANCE COMMON THEMES

• Culture of Compliance
• Research
  • Animal
  • Human
  • Export Controls
• Sexual Assaults/Title IX
• Conflicts of Interest
• Data Privacy
• Protection of Minors
PRIVACY COMMON THEMES

• Increased sharing of health information outside of Penn Medicine through HIEs and other arrangements.

• Growth of Penn Medicine through new acquisitions, requiring additional formality in Entity Privacy Officer program.

• Continued pressure from regulatory agencies through audits and enforcement activities on a range of HIPAA requirements.

• Roll-out of Web-based SPIA application tool to Schools/Centers to facilitate inventorying Confidential University Data and assessing controls in place.

• Proliferation of use of online educational services accessing student data that require privacy protections to ensure FERPA compliance.