NMSU’s Data is Highly Regulated

- Data Privacy Regulations (Major)
  - FERPA – Family Educational Rights and Privacy Act
  - HIPAA – Health Insurance Portability and Accountability Act
  - GLBA – Gramm-Leach-Bliley Act
  - RFR – Red Flags Rule of the Federal Trade Commission
  - FISMA – Federal Information Security Management Act
  - CUI – Controlled Unclassified Information (Executive Order 13556 – Effective November 14, 2016)

- Contractual Agreements
  - PCI DSS – Payment Card Industry Data Security Standards
  - Program Participation Agreement with the U.S. Department of Education (ED)... New FY18, Audit requirements to verify GLBA compliance and could affect institutional financial aid eligibility
HIPAA compliance at NMSU

NMSU Policies

• Chapter 15 | Information Management and Data Security

• 15.60 – Management of Health Information – HIPAA Compliance

• NMSU HIPAA Website

U.S. Department of Health & Human Services

• Health Information Privacy | HHS.gov

• HIPAA for Professionals
HIPAA background

• HIPAA Basics: Privacy, Security, and Breach Notification Rules

• The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provide individuals with certain rights to their health information.

• The Rules
  • **The Privacy Rule** sets national standards for when protected health information (PHI) may be used and disclosed
  • **The Security Rule** specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)
  • **The Breach Notification Rule** requires covered entities to notify affected individuals, U.S. Department of Health & Human Services (HHS), and in some cases, the media of a breach of unsecured PHI
HIPAA compliance

• What can I do?
  • YOU play a vital role in protecting the privacy and security of patient information. This presentation gives an overview of the rules, and it outlines the information protected by and who must comply with those rules.

• Definition of PHI
  • Protected Health Information (PHI) includes:
    – Any health information created, received, sent, or kept by the University.
    – Any information, in any form, that is related to the past, present, or future physical or mental health or condition of an individual; or payment for services.
    – Health and demographic information that can be used to identify an individual.

• PHI Comes in All Forms...
  • Spoken / Verbal Communications
  • Paper or “Hard Copy”
  • Electronic... locally stored on NMSU systems or Cloud Service Providers
Examples of HIPAA violations

• Improper use of Passwords and/or sharing account information. Examples may include but are not limited to:
  • Allowing a co-worker to use your login, or using a co-worker’s login, for any reason
  • Failure to report unauthorized use of an account or password belonging to someone else

• Getting into information outside the “minimum necessary to do your job,” and/or, outside your “professional need to know”...
  • (i.e., for personal reasons, out of curiosity [co-workers, high profile patients, family, etc.], and/or at the request of someone who cannot, or does not want to log on under their own account, etc.)

• Posting PHI or other personally identifiable data on the Internet (i.e., social networking sites)
Examples of HIPAA violations

• Attempting to avoid, or bypass the security mechanisms of any IT resources
• Illegally altering, destroying, or intentionally removing PHI or other private data from the University systems
• Selling health or personal information; or inappropriately selling/giving such information to the news media
• Transporting, taking home, or photocopying of protected health information
Information security and privacy are essential to help mitigate risk and protect our IT resources (computers, servers, and other electronic devices).

- Secure and protect your physical environment
- Create strong passwords and keep your computer accounts safe and secure
- Avoid computer security risks at work, home and on the road
- Understand violations and consequences
Report Unauthorized Disclosures

If you discover a potential disclosure, or if you become aware of someone not following information privacy and security policies...

- Report issue to your immediate supervisor
- Supervisor should report potential violation to the Chief Privacy Officer.

Note: Information Security and Privacy is Everyone’s Responsibility!!!
Questions?

Thank You For Your Time

Contact Information

Carlos Lobato – 646-5902
NMSU HIPAA Security Officer
Email: clobato@nmsu.edu

Robert Doyle – 646-5969
NMSU HIPAA Privacy Officer
Email: rdoyle@nmsu.edu