Secure IT Administration at NYS Psychiatric Institute

IT ADMIN ROLE-BASED TRAINING

Why more training

Numerous federal guidelines, including HIPAA and FISMA, require information security training with sufficient detail to cover roles you may serve

Organization-wide training doesn't address IT administration

NYSPI allows many programs to operate IT systems outside central IT (psyIT) management but requires consistent, secure administration

Consistency required for security of all programs in the shared environment

Exceptions are provided for those who have completed approved comparable training, such as CUMC's IT Custodian Training

Objectives

Review NYSPI policies, standards and procedures for IT systems and/or data management including:

- Systems Management
- IT Change Management
- Information Classification
- Identity Assurance, Account Management and Access Control
- Secure System Development Lifecycle (SSDLC)
- Data de-identification
- Incident Management

Provide resources for additional information

Provide reliable points-of-contact

High-level guidance

NYSPI is subject to all NYS policies and standards found at http://its.ny.gov/eiso/policies/security

NYSPI data, including data managed by NYSPI for CUMC, must be handled based on NYS standards unless more stringent standards (e.g. FISMA regulations) apply

NYSPI policies, procedures and bulletins merge NYS and CUMC baseline requirements

Any systems on any NYSPI network must comply with NYSPI policies and standards regardless of their function or data, even if the data is not NYSPI data (e.g. RFMH corporate data)

NYS Policies and Standards

Driven by NYS Information Security Policy NYS-P03-002

Based in federal NIST Special Publications (http://csrc.nist.gov/publications/PubsSPs.html)

Baseline from which to build on; standards are generally data-classification aware

NYSPI Systems Management Procedure

Four primary sections:

- Initialization,
- Maintenance,
- Logging/Audit and
- Account and Access Management

Exception request process also defined

Living document which will be updates as NYSPI needs evolve

System Development / Initialization

Supports responsible use of resources

Promotes standardization whenever possible

Encourages psyIT support where NYSPI's needs are greatest

Enhances inventory of systems and services

Ensures applicable support to minimize business and security risk

System Maintenance

References NYS and NYSPI patch management and change management processes

Keep systems at supported levels

Defines timelines for updates based on the importance of the system and severity of the issue (http://its.ny.gov/document/eiso/patch-management-standard)

Encourages discipline in changes

- Minimize unplanned outages
- Minimize wasted support resources
- Ensures recovery for failed changes is considered
- Ensures testing of change to avoid future surprises
- Informs overall Institute risk management

Logging and Auditing

Driven by system, data and/or program requirements

Ensures basic information required in the event of an incident are available and reliable

Encourages detection of the unexpected

Standardizes approach for “single-pane” view of network and systems

Account and Access Management

Promotes a consistent, consolidated, secure accounts

Recognizing increased risks with privileged accesses

Helps direct appropriate access to information

- Getting access consistently
- Keeping access and knowing how to access (“Which password was that again?”)
- Removing access when not needed

Promotes documenting access approvals

NYSPI Change Control

Leverage existing IT service request tools

Assigns responsibilities appropriately

Common changes are pre-approved and submitted as FYI

Change form helps busy staff learn from other's mistakes by planning key components

Helps limit conflicting changes

Expects and accounts for emergency and no/low-impact changes

Information Classification

Fundamental to overall IT controls in that different levels of protection and service are appropriate for different types of data

Establishes a standard for addressing information importance and for assessing NYSPI security

Ensures type of data is known and considered in system design and management

IT Controls directly tied in NYS and Federal regulation based on classification

See http://its.ny.gov/document/information-security-controls-standard or http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf for detailed controls and control families

Supports and enhances CUMC confidentiality-based classification scheme

Data Access Requirements

Confidentiality, Integrity and Availability requirements of data define Identity Assurance (Level of Assurance) requirements

Parallel's federal definitions to support federal grants and requirements

Supports cost-effective authentication and common, robust shared solutions to minimize impact on any one individual group

Data must be stored as required by classification; PHI/PII must be stored on encrypted storage

De-identification

Distinct from anonymous or coded data

Removal of all direct and indirect subject identifiers including the 18 HIPAA identifiers

Two methods:

- Statistical modification (e.g. encryption) such that information cannot be re-identified
- Removal of HIPAA identifiers
- See http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.htm

Coded data is identifiable via linking

- Coded data set should be stored separate from the linking file; ideally the linking file would be offline

Incident Management

Ensures appropriate prompt communication of events

Supports planning as well as response activities

Limits the need to define roles on the fly

Supports early reporting without negative impact of false positives

Questions

This training is not expected to address every need or situation. Please direct questions to the NYSPI IT Director or Chief Information Security Officer directly, via e-mail to psyIT-Admin@nyspi.columbia.edu or via the service desk.

Feedback on standards, services and this training are welcome.