RISK PROFILE

Information Management/Technology – Breach/Loss of Information

Intentional or unintentional breach or loss of information can expose organizations to loss of patient trust, potential fines, prosecutions, litigation, and reputational damage. Breach or loss of information may result from inadequate technical controls, inadequate administrative practices, information security awareness and cyber-attacks such as hacking, malware or ransom-ware attacks. This document contains information entered by HIROC subscriber healthcare organizations (acute and non-acute) in the Risk Register application to help you in your assessment of this risk.

Ranking/ratings[1]

- Likelihood – average score 2.75
- Impact – average score 3.80

The Risk Register allows for risks to be assessed on a five-point likelihood and impact scale, with five being the highest.

Key controls / Mitigation Strategies

- Information Technology (I.T.) controls
  - ✓ User authentication (e.g. multifactor authentication)
  - ✓ Unique user IDs, strong passwords
  - ✓ Role-based access controls for network, applications and processes within applications
  - ✓ Application installations restricted to administrator level only
  - ✓ Encryption of all external hard drives, USB keys, laptops and mobile phones
  - ✓ VPN with dual authentication
  - ✓ Intrusion detection and notification solutions
  - ✓ Firewall protection
  - ✓ Autoblock downloads
  - ✓ End point protection such as advanced threat detection and response and Data Leakage Prevention (DLP)
  - ✓ Email spam protection
  - ✓ Routine vulnerability scanning of the network and services
  - ✓ Network traffic analyzer and bandwidth utilization
  - ✓ Enhanced internet filtering protection
  - ✓ Penetration tests
  - ✓ Antivirus and antimalware solutions systems
  - ✓ Web and e-mail proxy servers to protect against malware and viruses
  - ✓ Timely application of security patches and software upgrades
  - ✓ I.T. documentation is electronic and stored off-site
  - ✓ Regular backups of data. Back-ups are archived to tape and moved to diverse physical locations to prevent loss due to catastrophic event (tapes moved offsite)
  - ✓ Secure records destruction

- Administrative, compliance and management practices
  - ✓ Regular audit (manual and system generated)
  - ✓ Assessments on new and existing critical information systems (privacy impact assessment, threat risk assessment, vulnerability assessment) with quarterly reports to internal and EHR collaboration related committees as well as annual security review.

Information Management/Technology – Breach/Loss of Information

- ✓ Formal privacy and information security policies and procedures with regular review (e.g. “lockbox”, breach protocols, acceptable use, mobile devices, social media, research, e-mail access and usage, etc.)
- ✓ Ongoing mandatory training, education and communication for all staff, volunteers, contractors and independent practitioners (e.g. education on phishing attacks, viruses, security and reporting, Cyber Security Awareness Month)
- ✓ Senior management accountability
- ✓ Regular review of the scope of cyber insurance coverage
- ✓ Privacy Officer and designated security lead roles to monitor and oversee organizational privacy and security activities
- ✓ Disaster recovery or Continuity of Operations Plan (COOP)
- ✓ Employee attestation of the organization’s privacy, confidentiality, code of conduct and security policies
- ✓ Human resource management for inappropriate access, use or disclosure
- ✓ Physical security of the building/organization
- ✓ Privacy Committee
- ✓ Regular reporting schedule to Senior Management Team and Board Committee on privacy program maturity

- Vendor management (e.g. contracts, due diligence)
  - ✓ Strong privacy and information management/security clauses in contracts
  - ✓ Vendor management practices for new systems always reviewed by IT
  - ✓ Centralized vendor management process
  - ✓ Assessment of vendor organization’s privacy and information security protocols
  - ✓ Vendor’s commitment to adherence to industry information security standards
  - ✓ Breach notification process
  - ✓ Vendor background checks
  - ✓ Clinical access agreements
  - ✓ Service level agreements with all vendors

Monitoring / Indicators

- System audits, password audits, high profile patient audits
- Network and server monitoring (e.g. daily morning, afternoon checks of servers)
- Auditing of PHI repositories
- Security audit conducted by external agency
- Regular review of logs (intrusion detection, firewall, e-mail, spam filter, active directory), active scanning and firewall monitoring
- Measure the maturity of the Information Security program annually
- Monitoring of real time global threats
- Incidents involving the following are monitored and reported:
  - ✓ Unplanned system downtime
  - ✓ Virus infection incidents
  - ✓ Breaches or unauthorized access
  - ✓ Complaints of privacy breach (including complaints to privacy commissioner’s office)
  - ✓ Lost USB keys, external hard drives, phones, etc. (with or without encryption)
  - ✓ Inappropriate use of internet

RISK
PROFILE

HIROC

Information Management/Technology – Breach/Loss of Information

- Multi-disciplinary representation in information security teams
- Staff training (frequency, attendance)
- Gaps identified from various assessments and progress over time (e.g. PIA, TRA)
- Dashboards for threat levels
- Bi-annual phishing campaigns results to assess employee awareness of phishing attacks
- Account file auditing
- Testing of recovery procedures
- Monitoring of back-ups
- Quarterly review of 3rd party (vendor) access to systems
- Building access logs
- Regular communications to enhance staff awareness is deployed and tracked

RISK REGISTER

[1]As of January 1, 2020
Note: information presented in this document has been taken from the shared repository of risks captured by HIROC subscribers participating in the Integrated Risk Management program.