RISK PROFILE

Regulatory – Privacy

Inadequate security practices for both paper and electronic information, loss/theft of personal health or personal information, privacy confidentiality complaints and/or lack of compliance with evolving privacy regulations/legislations pose significant risks for healthcare organizations. 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 3.00
- Impact – average score 3.44

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

- Roles and responsibilities:
  - ✓ Well established Privacy Officer role and a privacy committee to monitor and oversee privacy activities in compliance with regulations/legislations
  - ✓ Annual employee attestation of the organization's privacy, confidentiality, code of conduct and security policies
- Policies/procedures/protocols/programs:
  - ✓ Privacy policies/procedures/practices that cover the collection, use, disclosure, correction, retention and destruction of personal health information (PHI) and other confidential information (e.g. photos/videos for use in publications) including the use of "lockboxes", mobile devices, research privacy, etc.
  - ✓ Consent forms developed for the collection, use, and disclosure of PHI and other confidential information (e.g. photos/videos for use in publications)
  - ✓ Periodic review and revision of all privacy policy/procedures/protocols/consents to reflect up to date information
  - ✓ Privacy incident/breach response management plan
  - ✓ All privacy breaches and near misses reviewed by Privacy Officer and privacy committee for additional recommendations and oversight
  - ✓ Occurrence analysis and reporting for learning opportunities
  - ✓ Comprehensive privacy audit program
  - ✓ Internal and/or third party Privacy Impact Assessments (PIAs) and Threat Risk Assessment (TRAs) performed prior to implementing new or critical changes to the information systems
  - ✓ Privacy review of contracts and research study protocols
- Education/training:
  - ✓ Ongoing mandatory privacy training for all employees, residents, students, volunteers and contractors customized by roles and responsibilities (e.g. annual training, orientation), including education regarding:
    - Use of social media;
    - Shared systems including privacy component;
    - Consent for photos/videos used in publications (e.g. website, newsletter);
    - Privacy and security of PHI and health records in outpatient clinics, etc.

- ✓ Education/knowledge sharing in the form of:
  - PHI training modules;
  - Newsletter articles;
  - E-mails;
  - Team meeting education on a monthly basis;
  - Regional privacy meetings;
  - Ombudsman privacy workshop/conferences, etc.

- HR practices:
  - ✓ Human resources new hire protocols including sign-off of confidentiality agreement
  - ✓ Proper protocols followed when staff change roles to ensure role-based access rights are maintained
  - ✓ Stringent employment termination procedures (e.g. terminating access rights to systems, notifications to/from agencies and contractors of terminations)

- Information system/technology solutions:
  - ✓ Information technology controls (e.g. role-based access rights with management authorization, password protection, encryption, anti-virus system, internet and e-mail proxy servers, patch management, scanning software, and privacy warnings at system log-in)
  - ✓ Encryption of all external hard drives, USB keys, laptops and phones
  - ✓ Implementation of security tools and technology to protect against threats such as malware, spam, phishing e-mails, etc.
  - ✓ Implementation of systems that support required level of auditing
  - ✓ Confidential information locked in folders within the internal servers with limited access
  - ✓ Complexity required for passwords (e.g. minimum 8 characters) with a requirement to change every 90 days
  - ✓ Implementation of Artificial Intelligence (AI) privacy tools
  - ✓ Physical restriction from data centers that house the data
  - ✓ Implementation of online security/risk course for Information Technology (IT) department
  - ✓ IT security response team and plan

- External relationship management:
  - ✓ Partnership with associations and regulatory bodies to identify best practices and tools
  - ✓ Appropriate vendor management practices (e.g. confidentiality and non-disclosure agreements, and a review of agreements to ensure privacy language, roles and responsibilities of each party is clearly defined around privacy incidents/breaches)
  - ✓ Data sharing agreements detailing roles and responsibilities of each party
  - ✓ Additional cyber insurance coverage purchased and reviewed on a regular basis
  - ✓ Off-site storage vendors

- Physical security of paper records:
  - ✓ Health Information Management (HIM) department always locked with a service window
  - ✓ Review room is separate from where medical records are stored in the HIM department
  - ✓ Limited access to hardcopy records within short and long-term storage
  - ✓ External vendors needing access to chart storage area are accompanied by Security Guard

Regulatory – Privacy

- ✓ Directing staff to lock filing cabinets and desk drawers at night
- ✓ Operating fire suppression system to minimize risk of incineration
- ✓ Only short period of records (1 year for health files, and 2 years for finance files) are kept on site; all others are kept in long-term storage
  - Records maintained in long-term storage are on shelves within a no-traffic area;
  - Records are organized by destruction date, and category of content;
  - Destruction of records reviewed by Privacy Officer;
  - Scanning records for storage electronically

Monitoring / Indicators

- Number of privacy incidents/breaches and complaints, including the time required to achieve satisfactory resolutions
- Number of unplanned system downtime
- Number of completed confidentiality agreements, consent forms
- Tracking of staff privacy training records for new staff at orientation and all staff annually
- Audits of PHI systems, privacy policies/procedures, record destruction logs, user access to patient systems
- Completed PIAs and TRAs
- Results of vulnerability assessment and penetration tests conducted by IT
- Level of compliance with best practice security standards
- Information Privacy Commissioner (IPC) or Ombudsman reports, decisions and alerts
- Appropriate level of resources with privacy knowledge and background
- IT security monitoring
- Discharges audited on a monthly basis to ensure all charts are received by HIM department
- HIM staff monitor charts on a daily basis and the location of the charts are tracked at all times
- Regular review of media scans and social media
- Increased privacy assessments during COVID-19 pandemic as virtual and off-site clinical activities increased significantly
- Regular reporting through relevant committees to the board
- Quarterly privacy scorecard; maturity score assessment every 3 years
- Review and testing of disaster recovery plan

[1] As of January 1, 2021

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.