Cyber risks your organization may face:

- Identity theft resulting from lost or stolen PHI from medical records, Social Security or credit card numbers, driver’s licenses or financial information.
- Costly e-vandalism.
- Federal and state government lawsuits and investigations concerning PHI security breaches.
- Class-action claims resulting from breaches in your PHI data.
- E-business interruption due to a security failure or an Internet virus.
- Cyber extortion threats.
- Costs related to privacy notification, crisis management and disaster recovery.

The Solution: CyberSecurity by Chubb for Health Care Organizations

- Privacy notification expenses, including health care records monitoring and restoration.
- Privacy notification expenses provided on a voluntary basis.
- Premier privacy injury, including coverage for claims alleging actual or potential unauthorized access to the private information of natural persons, as well as the non-public information of third-party organizations.
- Coverage for written records breaches.
- Regulatory defense costs and fines, penalties and consumer redress associated with actual or potential unauthorized access to private information.
- Flexibility, with coverage provided on a reimbursement basis, or Chubb-controlled counsel and vendor selection.
- Number-of-affected-persons coverage outside the limit available for qualifying risks.
- Loss Prevention Consultant Services Reimbursement Program can reimburse a percentage of the cost of qualified cyber loss prevention services and referral resources to specialized cyber attorneys, vendors and service providers.
- Online network security risk assessment resulting in a comprehensive report of your company’s exposures (upon request).
- Combined third-party cyber liability and first-party cyber-crime expense coverages in one worldwide policy.

Why does your organization need cyber insurance?

- Stealthy external hacking of health care organization computer networks causes the majority of personal health information (PHI) data breaches today.1
- Any health care organization can be at risk under the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 or associated state laws. In fact, health care organizations account for more than 40% of all data security breaches reported across all industry segments nationwide.2
- Health care organizations face heightened regulatory scrutiny, increasing the scope of fines and penalties for health care data breaches.
The Solution: CyberSecurity by Chubb for Health Care Organizations (continued)

- Access to Chubb’s eRisk Hub®, an online risk management portal that can help your organization reduce the chance of a breach or loss occurring and bolster your incident response plan (IRP). This free resource also offers downloadable materials including a template IRP and Business Associate (BA) contract.

The cost of a health care data breach averages $316 per record, compared to $201 per record for all industry segments combined.³

Designed to do more

Chubb’s cyber solution for health care organizations is designed to address a wide array of risks associated with health care service delivery.

- Third-party cyber liability coverage for:
  - Disclosure injury, government and class-action lawsuits alleging unauthorized access to or dissemination of patients’ PHI.
  - Reputational injury, including suits alleging negligence in failing to keep PHI secure, libel, slander, defamation and invasion of privacy.
  - Impaired-access injury, including suits arising from system security failure resulting in your systems being unavailable to customers.
  - Content injury, including claims arising from copyright and trademark infringement.
  - Conduit injury, including claims arising from system security failures that result in harm to third-party systems.

- Optional first-party cyber-crime expense coverage for:
  - Privacy notification expenses (on a limit-of-liability or number-of-affected-persons basis), including the cost of credit, identity or health care records monitoring, and restoration services for affected customers.
  - Crisis management and reward expenses, including the cost of forensic and public relations expenses.
  - E-business interruption, including first-dollar extra expense.
  - E-threat, including the cost of a professional negotiator and ransom payment.
  - E-vandalism expense, even when the vandalism is caused by an employee.

Learn More
Contact your agent or broker today or visit Chubb online.

---