Cyber Liability Coverage: Health Care Facility Policy Forms

FAST **FACTS**

For more information, including current coverage provisions and eligibility, please contact our Underwriting department at (720) 858-6176 or email us: underwriting@copic.com.

State regulations and legal environments may limit the scope or availability of certain programs/resources. Please contact COPIC for details about your specific state.

Health care facilities face threats of data breaches (both from paper and electronic files) due to handling patient information such as medical records, social security numbers, dates of birth, and billing records. Data breaches result in reputational harm and sometimes significant financial costs. Other cyber threats can significantly impact medical facilities and their ability to effectively manage patient care.

COPIC includes cyber liability coverage with eligible policies to provide an added level of protection and offers resources to help implement preventative measures. The policy includes coverage for not only cyber-related events like phishing or ransomware, but also HIPAA breaches resulting from human error or inadequate policies and procedures.

SUMMARY OF COVERAGE AREAS*:

- **Unauthorized Access to IT Systems**—Coverage for a security failure to prevent unauthorized access of a computer system or a social engineering technique ('phishing' or 'pharming') that results in the alteration, copying, or deletion of data. Also includes the theft, loss or unauthorized disclosure of electronic/non-electronic confidential information, the transmission of malicious code or a computer virus, and a denial of service attack.
- **Defense Costs/Fines Associated with a Data Breach**—Coverage for regulatory defense costs and fines/penalties, when permitted by law, associated with violations resulting from a security or privacy breach of confidential, non-public information including (but not limited to) HIPAA and related state medical privacy laws, and federal privacy regulations for consumer information.
- **Data Breach Response Costs**—Coverage for reasonable and necessary fees/expenses incurred for a privacy breach response such as legal, forensic and investigation, public relations, voluntary notification, postage, related advertising, customer/patient support, reporting to administrative agencies, and credit monitoring.
- **Damage to Network Assets and Interruption Expenses**—Coverage for reasonable and necessary expenses to replace, recreate, or restore digital assets after computer hardware or computer systems are damaged, destroyed, or stolen. Also includes business interruption and extra expense coverage for income loss as a result of the total or partial interruption of the insured's computer system.
- **Cyber Extortion**—Coverage for extortion expenses as a direct result of a credible threat that involves (including, but not limited to) the release or destruction of confidential information related to unauthorized access to a computer system, damage to or restricting access to a computer system, the introduction of malicious code, and electronic communication with customers while falsely claiming to be the insured.
- **Cyber Terrorism**—Coverage for income loss and interruption expenses as a result of a total or partial interruption of a computer system due to a cyber terrorism attack.
- **PCI DSS Assessment**—Coverage for the fines and penalties levied by the Payment Card Industry Data Security Standards Council against merchants who are not PCI DSS compliant.
- **Online or Print Media Claims**—Claims alleging libel, slander, invasion of privacy, emotional distress, plagiarism, piracy, copyright or trademark infringement, and domain name infringement.

COVERAGE AGREEMENTS:

Subject to the limits of liability applicable to the *Supplemental Cyber Liability Coverage Booklet*, the cyber liability coverage will pay defense costs, fines and penalties, expenses, and/or losses resulting from a claim for any actual or alleged incident(s), provided that*:

1. Such claim is first made against you during the policy period and occurs after your retroactive date;
2. You report such claim in writing during the policy period (and within the specified number of days from which you first discover the incident); and
3. The incident is directly caused by and/or directly resulted from a covered cause of loss.

**This is a general overview of the coverage and certain terms and conditions apply based on the specific claim and/or incident. Please review the Supplemental Cyber Liability Coverage Booklet for full details including a list of exclusions related to your coverage.*

BASIC LIMITS OF LIABILITY:

Insured Hospital or Facility—$100,000 each claim // Annual Aggregate Limit: $100,000

- Multimedia Liability
- Security and Privacy Liability
- Privacy Regulatory Defense and Penalties
- Privacy Breach Response Costs, Patient Notification Expenses, and Patient Support and Credit Monitoring Expenses
- Cyber Terrorism Coverage
- Cyber Extortion Coverage
- Network Asset Protection

INCREASED LIMITS

Medical facilities may want to consider added levels of cyber liability protection. Cyber crime is on the rise, especially with the growing number of connected devices to business networks, and can come with significant costs. Additionally, fines and penalties for data breaches and costs of ransomware events are also on the rise. COPIC offers increased limits of liability—a flexible option without the hassle of having to add a separate policy.

RESOURCES AVAILABLE ON COPIC'S WEBSITE

As part of your coverage, you have access to a risk management website portal from our cyber liability insurance partner. This portal offers a number of resources and tools that can assist with the prevention and management of cyber risks including incident response and IT security planning resources, sample policies and procedures, online training resources, risk assessment tools, and information on cyber trends and other news. You can access this information at https://www.callcopic.com/cyber-resources.

The information previously listed regarding provisions of cyber liability insurance coverage is provided for descriptive purposes only. Changes in coverage provisions and eligibility may have occurred since publication; provisions and eligibility currently in effect take precedence.