CHUBB®

Cyber Claims Scenarios

for Healthcare Organizations

Risk	Industry	Business	Claim Difference
Loss of PHI	Healthcare	Commercial	Top-Tier Response Coach and Forensic Firm
Physician Impersonation	Healthcare	Commercial	Expert Claims Investigation
Ransomware Attacks	Healthcare	Commercial	Technical Expertie
Vendor/Supply Chain	Healthcare	Commercial	Top-Tier Response Coach and Forensic Firm

Claim Scenario Details

It is believed that criminals from outside the U.S. were able to exploit vulnerabilities in the Insured's system to access more than 200,000 patients' PHI.

Loss of PHI

A healthcare organization was informed by law enforcement that its patients' information was found on the dark web. It is believed that criminals from outside the U.S. were able to exploit vulnerabilities in the Insured's system to access more than 200,000 patients' PHI (personal health information). Chubb assisted the Insured by retaining an incident response coach and a forensics firm from our cyber panel. Several governmental/regulatory agencies were notified with the assistance of the coach. A call center was established and credit monitoring was offered to the affected patients.

Physician Impersonation

An Insured healthcare organization was notified by an outside firm that one of its doctors was being impersonated by an unlicensed physician posing as him. This imposter was able to review several medical files as part of a physician peer review process. Once the Insured became aware of the situation, it had to notify patients whose PHI (personal health information) was inappropriately exposed to this person. Several of the affected individuals have brought third party claims against the Insured for failing to safeguard their PHI.

An Insured healthcare organization was notified by an outside firm that one of its doctors was being impersonated by an unlicensed physician.

Claim Scenario Details

Ransomware Attacks

A hospital's computer system was the subject of a ransomware attack. While the attacker sought only $500, the cyberattack essentially shut down the medical facility. The hospital incurred significant expenses attempting to restore the data from their computer systems. They could not bill any of the health insurance carriers while the system was affected. Additionally, the imaging capabilities of the hospital were greatly impacted as they could not produce the images from MRIs or CT scans. The malware completely corrupted the hospital's system and they had to resort to paper mode to chart and monitor patients. Lastly, the hospital's payroll system also went down as part of the attack. As a result of the attack, more than $700,000 was paid for forensics, data recovery, business interruption and crisis management costs.

The malware completely corrupted the hospital's system and they had to resort to paper mode to chart and monitor patients.

As a result of the incident, the Insured incurred $20,000 in first party costs.

Vendor/Supply Chain

A business associate of the Insured fell victim of a ransomware attack that encrypted many of its files. The business associate possessed medical records and personal health information of the Insured's customers and had to retain an incident response coach and forensic firm to remedy the ransomware attack on its system. While our Insured had previously utilized Chubb's pre-incident services to better prepare for a breach, the Insured still needed to consult with its own incident response coach from our cyber panel to determine what reporting obligations it had under HIPAA. The incident response coach eventually determined that there was no exfiltration of personal health information from the business associate's system. As a result of the incident, the Insured incurred $20,000 in first party costs.

Contact Us

For more information on Chubb Cyber insurance solutions, visit www.chubb.com/cyber.

Chubb. Insured.℠

Form 30-01-0096 (Ed 7/19)