# Healthcare

## Effective cyber breach protection for the healthcare industry.

Essentially, a cyber breach is not a question of "if." The only question is "when?"

Information exposures are difficult to control and are subject to many different types of loss events. And even with the best systems, controls, personnel and procedures, no organization is immune to the risk. It only takes one small human error, a simple property crime, or one clever hacker, to compromise millions of patient records, or otherwise wreak havoc on your organization.

### Significant exposure

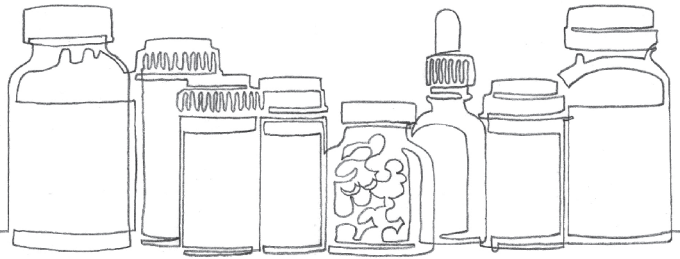
The scale of protected health information (PHI) maintained by healthcare organizations and the digitization of electronic health records have increased the vulnerability to large breaches. Compulsory breach notification laws provide a great deal of exposure. In addition to the patchwork of state laws affecting all businesses, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) operate at the federal level. These laws require time-consuming and labor-intensive internal investigations, specialized outside vendors, and can often disrupt a healthcare organization's ability to prioritize patient care.

**242.6m**

personal records in healthcare were compromised between 2005 and 2018
Source: www.privacyrights.org

**31%**

of healthcare breaches in 2018 were attributed to hack or malware
Source: Breaches reported to BBR Services



## Class action lawsuits

The publicity and patient dissatisfaction that surround a data breach have spurred a wave of class action complaints against organizations big and small. Relying on a variety of medical privacy laws, enterprising plaintiffs' lawyers have filed complaints seeking billions of dollars in damages. The specter of such damages, and the sizeable costs of litigation, often push organizations to settle even in the absence of any clear harm to the affected patients.

## Regulatory investigations and penalties

State and federal regulators have made one point clear: a significant breach of patient information will result in monetary penalties, onerous corrective action plans, and ongoing audits. Whether through the strict data privacy and security requirements of HIPAA/HITECH, or the increasing interest of state attorneys general in enforcing medical privacy laws, the regulatory landscape for healthcare organizations carries an immense amount of risk. Regardless of any legal liability, a cyber breach greatly increases the risk of reputational and brand damage.

## Why Beazley

Beazley, a leading insurer of technology and information security risks, has developed BBR, a solution to privacy breaches and information security exposures tailored to the needs of healthcare organizations.

BBR is a complete privacy breach response management and information security insurance solution, which includes a range of services designed to help you respond to an actual or suspected cyber breach effectively, efficiently, and in compliance with the law.

"We greatly appreciate Beazley's Breach Response services and the efficiency and knowledge that is available to us when we need it the most."

Large multi-facility healthcare system

## Coverage

**Breach response**
- Legal services
- Computer forensic services
- Notification services for up to five million affected individuals
- Call center services
- Credit monitoring, identity monitoring or other personal fraud or loss prevention solutions
- Public relations and crisis management expenses
- All of the policy's multiple limits will be available for breach response.

**First-party**
- Business interruption loss from security breach or system failure
- Dependent business interruption loss from security breach or system failure
- Cyber extortion loss
- Data recovery loss
- Data and network liability.

**Third-party**
- Third-party information security and privacy coverage with up to $15 million
- Full media liability
- Regulatory defense and penalties
- Payment card liability and costs.

**eCrime**
- Fraudulent instruction
- Funds transfer
- Telephone fraud.

**Criminal reward**

Cyber breaches take many forms. External hackers and malicious insiders cause many breaches, but did you know that simple carelessness is responsible for a surprisingly large number of breaches?

Every breach is different. It is important to work with a partner who has been there before.

## BBR Services

Beazley is unique among insurers in having a dedicated business unit, BBR Services, that focuses exclusively on helping clients manage cyber breaches successfully. In each case BBR Services collaborates with you to establish the best response that is tailored to your individual needs.

They coordinate the carefully vetted forensics experts and specialized lawyers to help you establish what's been compromised; assess your responsibility; and notify those you have to. In addition, BBR Services coordinates credit or identity monitoring for your customers and offers PR advice to help you safeguard your reputation.

BBR Services also provides a full range of resources to help mitigate risks before an incident occurs. On our Beazley owned and managed risk management portal, beazleybreachsolutions.com, you will find resources for incident response planning, employee training, compliance, and security best practices. Newsletters and live expert webinars educate you about the latest threats, preventive steps, and regulatory developments. BBR Services also coordinates a variety of pre-breach services such as onboarding calls, incident response plan reviews and on-site workshops, so you can improve the robustness of your cybersecurity.

## Case studies

**Insider**

- A healthcare organization's employee posted patient treatment information on a social media website. The employee did not include the patient's name, but because the disclosure occurred in a small town, the public could determine the patient's identity. BBR Services connected the organization to expert privacy legal counsel, who provided advice on notification to the individual, as well as satisfying the necessary regulatory response.

**Hacking and malware**

- A healthcare organization was subjected to a sophisticated foreign phishing attack, which exposed information in employee email boxes of nearly 20,000 pediatric patients. Employees had clicked on the phishing emails and either gave up credentials or launched malware into their network. Forensics found some evidence of data exfiltration. The data contained patients' names, clinical information, phone number, addresses, insurance information and some Social Security numbers. BBR Services coordinated outside legal counsel, forensics, notification, a call center vendor, and credit monitoring. An Office for Civil Rights (OCR) investigation is pending.

**Physical loss/non-electronic records**

- Imposters posing as an x-ray disposal vendor stole barrels of x-ray films from a hospital loading dock. The hospital's employees did not ask for identification, nor did they question why the vendor's employees were not in their usual truck and uniforms. The stolen barrels contained several hundred patient x-rays. The hospital worked with BBR Services and panel counsel to draft notification letters, frequently asked questions and a media statement.

## Case studies

**Inadvertent disclosure**

- An IT vendor had inadvertently unsecured a file containing over 30,000 patients' billing information, such that it was searchable on the internet using search engines such as Google. The hospital discovered the incident during security testing when a larger healthcare system acquired the hospital. The information exposed included names, Social Security numbers, dates of birth, addresses, treatment information, and insurance information. The hospital utilized outside legal, forensics, notification services, a call center, credit monitoring and crisis management. The hospital was investigated by OCR and four attorneys general.

**Missing portable device**

- Unencrypted back-up tapes were lost that contained 1.6 million pediatric patients' billing information including names, dates of birth, Social Security numbers, diagnosis codes and health insurance information. The tapes also included employees', physicians' and vendors' information totaling 200,000 individuals. The tapes were believed to have been lost during a remodeling project in the IT department. The healthcare entity used a notification vendor, a call center, credit monitoring, legal, forensics and crisis management, all which were coordinated by BBR Services. There was an OCR investigation that lasted 3.5 years and was ultimately dismissed.

**Stolen portable device**

- A laptop was stolen from a physician's office. The thief, impersonating a construction worker, entered the physician's office area when the hospital was undergoing an expansion. The laptop was one of a few that was unencrypted, as it was bought with departmental funds outside of the normal procurement process and did not go through IT for encryption. The laptop contained pediatric patients' names, treatment information, and diagnosis. BBR Services was contacted and assisted with outside legal counsel. An OCR investigation lasted for four years and was ultimately dismissed.

"Under the stress of dealing with a large security incident, Beazley was a calm partner. They were responsive, efficient, extremely easy to work with and connected us with a variety of experts who assisted us every step of the way."

E. Ward Begley II, General Counsel and Roz Cordini, Chief Compliance Officer
Owensboro Health

beazley



BZCER001_US_01/19