

Healthcare

Effective data breach protection for the healthcare industry.

Essentially, a data privacy 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 organisation 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 organisation.

Significant exposure

For healthcare establishments the confidentiality of private patient records is a primary concern. The advent of paperless filing and electronic communications, as well as advances in new technology, all have the potential to seriously impact data security.

Stolen healthcare records are worth on average five times more than credit card details on the black market and the regulations surrounding the reporting of healthcare data breaches are onerous.

Beazley insures more than 500 healthcare providers against data breach risk and has helped more than 2000 healthcare clients manage breaches successfully. Our dedicated business unit, BBR Services, marshals the expert services that healthcare providers need to handle data breaches with confidence while our third party claims experts help clients defend themselves against potentially costly lawsuits.

43m

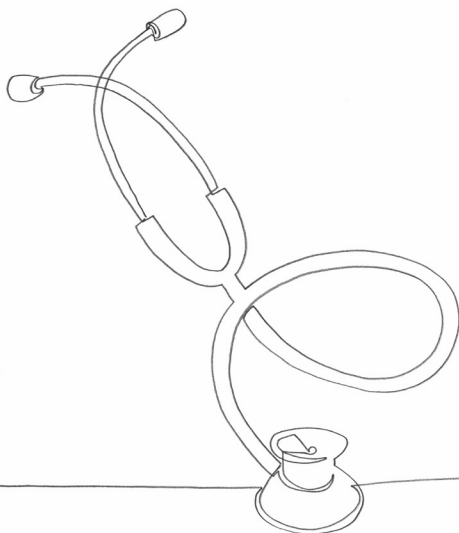
personal records in healthcare were compromised between 2005 and 2015

Source: www.privacyrights.org

27%

of breaches recorded between 2005 and 2015 are healthcare

Source: www.privacyrights.org



Healthcare

Regulatory investigations and penalties

Compliance with the UK's Data Protection Act (DPA) is not just about the confidentiality of personal data, it is also about information security and ensuring that data is securely stored and managed.

The Information Commissioner's Office (ICO) has several options when it finds that an organisation has breached the UK Data Protection Act. A significant breach of personal data could result in actions including issuing monetary penalties, enforcement notices, auditing and prosecutions.

In March 2015, North Tees and Hartlepool NHS Foundation Trust was ordered by the ICO to review its data protection policy after a file containing sensitive patient information was found at a bus stop. It was one of a number of data loss incidents over the last year, examples of which include reports containing patient data being sent to the wrong people.

No matter the industry sector or size, if an organisation fails to comply with data protection regulation the consequences can be severe, from reputational and share price damage, to hefty fines up to £500,000 and even criminal charges.

*Source: www.ico.org.uk

“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

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 organisations.

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 data breach incident effectively, efficiently, and in compliance with the law.

Beazley's client list includes 29% of Healthgrades' top hospitals in the US and more than a third of the 16 US News & World Report's honor roll hospitals (2015 rankings). A third of Beazley's Breach Response policies have to date been taken out by healthcare organisations.

Third party coverage

- Third party information security and privacy coverage with up to €25m/£15m in limits in addition to the breach response coverage
- Regulatory defense and penalties
- Website and offline media liability
- PCI fines, penalties and assessments*
- Cyber extortion
- First party business interruption and data protection with limits up to €25m/£15m.

* Where insurable by law

The logo for Beazley, featuring the word "beazley" in a lowercase, serif font with a thin black outline around the letters.

Data 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 data breaches successfully. In each case BBR Services collaborates with you to establish the best response that is tailored to your individual needs.

BBR Services is a dedicated team of data breach professionals who assist BBR policyholders at every stage of incident investigation and breach response.

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 PR advice to help you safeguard your reputation.

Insider

- A healthcare organisation'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 organisation 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 organisation was attacked by 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 centre 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.

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, date of births, addresses, treatment information, and insurance information. The hospital utilised outside legal, forensics, notification services, a call centre, credit monitoring and crisis management. The hospital was investigated by OCR and four attorneys general.

Missing portable device

- Unencrypted backup tapes were lost that contained 1.6 million pediatric patients' billing information including names, date of births, 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 centre, 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, impersonated as 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 4 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