Data Breaches

Jeffrey S. Gelburd, Vice President
Program Administrator
Murray Securus

What is a data breach?

A loss involving theft, accidental release or accidental publication of Personally Identifiable Information (PII) or Protected Health Information (PHI) including:

- Social Security number
- Bank account, credit or debit number
- Driver's license number
- PIN numbers
- Medical diagnosis, patient history and medications
- Other private information defined by state or federal law

How can a data breach occur?

- Unauthorized access (such as by former employees, vendors or hackers)
- Stolen or lost paper files, or shipped documents failing to arrive at proper destination
- Mailing, faxing or emailing documents with one person's PII to the wrong person
- Computer system hacked by virus, Trojan horse or improper security
- Stolen or lost laptop, computer disks, USB flash drives, portable hard drives or back-up tapes
- Employee error or oversight

Who needs this coverage?

Virtually no business is immune from this potential risk including yours. Nearly all businesses that handle or store any private business, customer or employee data is at risk for a data breach and could benefit from this coverage. The possibility is especially high for organizations that routinely deal with credit cards, patient medical records, Social Security numbers and other sensitive information including:

- Professional Services (lawyers, accountants, real estate , insurance agents)
- Retailers and restaurants
- Financial services
- Healthcare Providers/Facilities
- Educational Institutions
- Manufacturing or Distributors

Isn't this covered by one of my other policies?

Not likely. There are times when pieces of privacy coverage show up on other policies, but that coverage and those triggers are generally not as broad. It is also very important to have a standalone policy to make sure you have complete coverage not only for defense costs and liability, but also for notification and credit monitoring costs.

What if I lose information but don't get sued, do I still need coverage?

Yes. This policy provides coverage for preventative costs including notification and credit monitoring, as well as upfront costs like data forensic and crisis management expenses. If you do get sued, there is also coverage for defense and indemnity expenses.

What are Notification costs?

Notification costs are the costs of creating and sending a letter to clients and/or employees who have had their information compromised. **This is required by 46 states currently**. A single letter can cost from $1-$5 per person.

What are Credit Monitoring Costs?

Credit Monitoring Costs are the costs to pay a credit bureau to monitor someone's credit. These costs can be very expensive, ranging between $20-$30/person per year.

What are data forensic expenses?

These are the costs to pay an expert to figure out how your network was hacked/how the data was compromised.

What are crisis management expenses?

These are the costs associated with public relations damage control when you have lost information and/or have had a breach.

Does this cover HIPAA, HiTECH, FTC and Graham-Leach-Bliley (fines)?

Yes, it does. It also covers you for other privacy-related fines, including state-mandated fines.

Does this cover loss of employees' information, not just client information?

Yes

Am I covered if my employees lose or steal client information?

Yes, as long as they are not Executive Officers of the company
.

MURRAY SECURUS

If you have questions about how to better protect your data, contact Jeffrey S. Gelburd at jgelburd@murrayins.com or 717.620.2476.
Risk Management • Insurance • Health Benefits • TPA • Wealth Management • HR • murrayins.com