This year’s Verizon Data Breach Investigations Report (DBIR) is based around nine incident classification patterns: common signatures that describe the vast majority of security incidents. Just three of these nine patterns cover a significant 73% of security incidents experienced by healthcare organizations. Improving your defenses against these three areas could make your organization, and your patients’ data, much more secure.

**PHYSICAL THEFT AND LOSS**

46% of all the security incidents in our dataset that targeted healthcare organizations were thefts or losses of “information assets” — for example laptops, USB drives, paper files, and backup discs. This doesn’t include situations where files and hard drives are improperly disposed of; these incidents come under Miscellaneous Errors.

Healthcare organizations suffered far more from theft and loss than any other industry in our dataset. While some of this is no doubt due to higher standards of disclosure reporting in healthcare versus other industries, the types of environments where data is used in this industry are also likely to contribute.

Doctors’ clinics, hospital wards and reception areas are all bustling places where computers and paper files are constantly on the move, visitors freely move around, and staff are prone to distraction by a sudden emergency. In such circumstances, assets are vulnerable to loss or theft.

What you can do

- **Encrypt devices.** While encryption won’t affect the chances of an asset going missing, it will protect the data it stores.
- **Back it up.** Regular backups can prevent the loss of valuable data, reduce downtime, and help with forensics should you be breached.
- **Lock it down.** Secure IT equipment to immovable fixtures, and store sensitive assets — including paper documents — in a separate, secure area.

Data breaches can be extremely costly. The Verizon DBIR has, for years, been the best source of insight about the threat landscape. This year’s report covers over 63,000 security incidents from 95 countries.
INSIDER MISUSE

Insider and privilege misuse accounted for 15% of incidents suffered by healthcare organizations.

This category covers situations when employees, ex-employees and partners with access rights use their privileges to access data, either in person or over the network.

Culprits can come from every level of the organization, even senior executives.

In healthcare there’s not only patient medical data to worry about, but potentially valuable intellectual property such as clinical trial findings, and customer payment details too.

While physical loss and theft dominated healthcare security incidents overall, most incidents of insider misuse were digital. Rather than sneaking paper files out in a bag, insiders used the corporate network 85% of the time. With the right credentials, it’s easy to copy files to a USB drive without anyone noticing.

What you can do:

- **Know your data.** The first step in protecting your data is knowing where it is and who has access to it.
- **Review user accounts.** Having identified who has access to sensitive data, implement a process to continuously monitor user and system behavior as well as revoking access when employees change role or leave.
- **Watch the exits.** Set up controls to watch for data transfers out of the organization.
- **Publish anonymized results of audits.** Enforcing policies as part of a continuous monitoring program can be a powerful deterrent.

MISCELLANEOUS ERRORS

12% of healthcare incidents in our dataset fall under Miscellaneous Errors. This category covers any mistake that compromises security, primarily:

- Posting of private data to public sites
- Sending of information to the wrong recipients (whether in the post or by email)
- Failing to dispose of assets securely — e.g., by shredding paper or wiping hard drives

The public is rightly sensitive about healthcare data, and any leakage is a potential PR crisis in the making.

While it’s impossible to entirely stop human error, you can reduce the potential damage through changes to controls and technology.

What you can do:

- **Implement DLP.** Consider implementing data loss prevention software to block sensitive information being sent by email.
- **Strengthen controls on publishing.** Decrease the frequency of publishing errors by tightening controls around posting documents to websites. Regularly scan public-facing sites for sensitive data.
- **Train staff about asset disposal.** They must understand that documents and computers can’t just be put in the bin.

HOW CAN WE HELP?

We put our unique security insight to work every day in the solutions we provide. Our products and services can help you guard against the threats you face.

- **Our Data Loss Prevention (DLP) and Data Discovery, Identification and Security Classification (DDISC) services can help you stop sensitive data leaving your organization** — whether accidentally thanks to user error, or deliberately due to misuse.
- **Our Identity and Access Management services give you better control over user credentials, reducing the risk of insider misuse.** You can enforce two-factor authentication and quickly revoke privileges when an employee leaves.