

West Virginia Executive Branch Privacy Tip

Question:

Security breach or data breach...Is there a difference?

Answer:

A “security breach” is generally defined as an “unauthorized access to and acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”

A “data breach” is generally defined as an unauthorized disclosure or mismanagement of information that compromises the security, confidentiality, or integrity of personally identifiable information (PII), such as Social Security numbers, name and addresses, date of birth, health care information and bank account information.

The term defined in the WV OT Information Security Policy is **Security Incident** – An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

These terms are used interchangeably and reference various forms of information security breaches which generally include:

- A hacker breaking into a network and stealing information.
- A lost or stolen laptop that has someone's social security number.
- A lost blackberry that has personal information about employees or customers.
- A fax that includes financial information that's thrown away instead of shredded.
- Theft of sensitive or confidential information by employees.

Sources cited:

National Institute of Standards and Technology

CMS – HIPAA Security Rule

WVOT Information Policy