

# TOP 6 HIPAA ePHI EXPOSURES

## Unsecured/Unencrypted Data

- Store all ePHI encrypted at rest
- Encrypt all sensitive information in transit
- Know your current policies and procedures



## Hacking & Phishing for Data

- Only open emails and attachments from known senders
- Don't share usernames and/or passwords
- Notify your security team immediately if something happens



## Loss/Theft of Laptop or Device

- Password protect and encrypt devices containing ePHI
- Never leave your laptop, cell phone or other mobile device unattended
- Alert your security team as soon as something goes missing



## Lack of Employee Training

- Know your requirements under the HIPAA standard
- Ensure all employees understand the proper handling of ePHI
- Regularly review policies and communicate changes to all personnel



## Unauthorized Use or Sharing of ePHI

- Ensure Business Agreements are in place before sharing protected information
- Protect ePHI in your care according to policies and standards
- If unsure, contact your Compliance Officer



## Improper Disposal of ePHI

- Confirm that all ePHI is properly classified and stored according to Data Storage and Retention policies
- Properly dispose of sensitive documents after retention periods expire
- Consult your Compliance Officer before disposing of hardware used to store protected information



## TO PROTECT FROM THESE EXPOSURES...

To learn more about building a healthcare security and compliance program, go to

[www.sans.org/sec474](http://www.sans.org/sec474)