
# TLP: WHITE: ASPR/CIP HPH Cyber Notice: Meltdown and Spectre Vulnerability Guidance UPDATE #1

**January 17, 2018**



Healthcare and Public Health Sector partners-

The attached report is a technical update to the previously distributed HPH Cyber Notice covering chip vulnerabilities named Meltdown and Spectre. Both Meltdown and Spectre are vulnerabilities in how computer chips handle data that have the potential to expose sensitive information, such as protected health information (PHI), being processed on the chip. As this information is protected from disclosure under HIPAA, Healthcare and Public Health (HPH) entities should employ risk management processes to address these vulnerabilities and ensure the security of medical records and other PHI.

Major concerns for the HPH sector include but are not limited to:

- Challenges identifying vulnerable medical devices and accessory medical equipment and ensuring patches are validated to prevent impacts to the intended use.
- Cloud Computing: Potential PHI or Personally Identifiable Information (PII) data leakage in shared computing environments
- Web browsers: Possible PHI/PII data leakage
- Patches: Potential for service degradation and/or interruption from patches

The detailed report can be found here: Technical Report on Widespread Processor Vulnerabilities

Regards,

The ASPR Critical Infrastructure Protection Team

If you have any questions, please contact us at cip@hhs.gov.