RobbLAW
An IT Security and Compliance Law Firm

# Health Insurance Portability and Accountability Act

## HIPAA Structure

- **Privacy Rule**
- **Security Rule** (*Required or Addressable*)
    - Administrative Safeguards
    - Physical Safeguards
    - Technical Safeguards
- **Final Omnibus Rule Update** (extends Privacy and Security rule for HITECH)
    - **Defined Terms**
        - **SECURITY INCIDENT** is defined as "*the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.*"
            - 5 C.F.R. 164.304
        - **BREACH** is defined as "*the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.*"
            - 45 C.F.R. 164.402

## HITECH Structure

- Requires "**meaningful use**" of Electronic Medical Records
- **Subtitle D**
    - Extends Privacy and Security Rule to Business Associates and requires BAA
    - Report breaches of > 500 individuals to HHS

## Organizations

- US Department of Health and Human Services (**HHS**)
- Office of Research Integrity (**ORI**)
- Office of Civil Rights (**OCR**)

## Protected Health Information (PHI) Identifiers:

1. Names
2. Geographical Identifiers Smaller Than A State (except for the initial three digits of a zip code)
3. Dates (other than year) Directly Related To An Individual
4. Phone Numbers

5. Fax Numbers
6. Email Addresses
7. Social Security Numbers
8. Medical Record Numbers
9. Health Insurance Beneficiary Numbers
10. Account Numbers
11. Certificate / License Numbers
12. Vehicle Identifiers and Serial Numbers (including license plate numbers)
13. Device Identifiers and Serial Numbers
14. Web Uniform Resource Locators
15. Internet Protocol (IP) Address Numbers
16. Biometric Identifiers (including finger, retinal, and voice prints)
17. Full Face Photographic Images and Any Comparable Images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data