HIPAA Quick Facts



COMMON VIOLATIONS



- · Lost or stolen devices
 - leave PHI vulnerable
- Unauthorized access



- by employees to PHI without a work-related reason
- 'snoopina'





- of records, such as unshredded paper files or notes in open trash
- of specimen containers with PHI in open trash

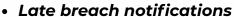


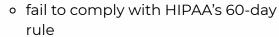
- Inadequate staff training
 - on handling PHI securely and HIPAA policies



No HIPAA risk assessments

- or failure to address identified security risks
- Lack of encryption
 - puts PHI at risk if devices are lost







- Unauthorized filming or photographing patients
 - compromises patient privacy



- Data exposure when working from home
 - do not leave paperwork or devices unattended





 de-identified information must be used in presentations, publications, trainings, or websites, unless consent is obtained.



- sent to the wrong recipient
- sent to personal e-mail accounts outside of the organization

MORE RESOURCES: HTTPS://OSUMC.SHAREPOINT.COM/SITES/PRIVACY

18 PHI Identifiers

- 1. Name
- 2. All geographic subdivisions smaller than a state
- 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- 4. Phone numbers
- 5. Fax numbers
- 6. E-mail addresses
- 7. Social security numbers
- 8. Medical record numbers
- 9. Account numbers
- 10. Health plan beneficiary numbers
- 11. Certificate/License numbers
- 12. Vehicle identifiers (numbers)
- 13. Device identifiers
- 14. Web URLS
- 15. IP address
- 16. Biometric identifiers
- 17. Full face photographic images
- 18. Any other unique identifying number, characteristic, or code



