Office of Civil Rights Penalty Caps for HIPAA Violations

Protected Health Information (PHI): Information that can identify a patient and relates to the patient's health condition, treatment or payment for treatment. There are 18 elements of PHI.
ePHI: PHI received, created, maintained or transmitted in electronic form.

Culpability	Minimum Penalty for Violation	Maximum Penalty Per Violation	Annual Limit
No knowledge	$100	$50,000	$25,000
Reasonable Cause	$1,000	$50,000	$100,000
Willful Neglect-Corrected	$10,000	$50,000	$250,000
Willful Neglect-Not Corrected	$50,000	$50,000	$1,500,000

For research purposes, how do we protect against HIPAA violations and maintain compliance?

- All data collection should occur on Ascension St. John or Ascension St. John-associated facility premises.
- Only the study investigators listed on the "team list" or "delegation log" may have access to the research data (IRB Form A-2).
- Paper data collection sheets should be stored in a locked file cabinet when not in use; paper data collection sheets should never be removed from the premises.
- All electronic data must be stored on an Ascension St. John network, password-protected, encrypted computer drive (i.e. the H: drive or the Microsoft OneDrive). No patient data should ever be stored on the hard drive of a personal computer.
- If data are emailed, email encryption must be used. Ascension employees, residents and fellows should always use their Ascension email address when emailing data.
- Emails from one Ascension address to another Ascension address are encrypted.
- If you need to email data to a non-Ascension email address, you must put -phi- or -secure- in the subject line to encrypt the email.

Elements of PHI[1]

- Names
- All geographic divisions smaller than a state, including city, county, precinct, zip codes and their equivalent geocodes, except for the first three digits of the zip code, if according to the current publicly available data from the Bureau of the Census:
    - The geographic unit formed by containing all zip codes with the same three digits contains more than 20,000 people; and
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates that are directly related to an individual, including birth and death date, admission date, discharge date, death date 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 single category of age 90 or older.
- Telephone numbers
- VINs and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- URLs
- Social security numbers
- IP addresses
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers (i.e. FINs)
- Any other unique identifying number, characteristic or code
- Certificate/license numbers

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected