KNOW THE 18 IDENTIFIERS OF PHI

WHY IT MATTERS

If the information can identify a resident, it is considered Protected Health Information (PHI)—and it must be safeguarded.

Name - Full name or last name with initial

Address - For example city, county, zip code

Dates - Any dates related to a resident (e.g., birthdate, admission date, discharge date, date of death)

Phone numbers - Resident or family contact numbers

Fax Numbers - Any fax number linked to resident records

Email Addresses - Personal or work emails associated with the resident

Social Security Numbers - Complete or partial SSNs

Medical Record Numbers - Any facility-generated medical record identifiers

Health Plan Beneficiary Numbers - Medicare, Medicaid, or private insurance identifiers

Account Numbers - Any financial accounts related to the resident's care

Certificate/License Numbers - Includes professional licenses or certifications

Vehicle Identifiers & Serial Numbers - License plate numbers or vehicle details

Device Identifiers & Serial Numbers - Medical devices linked to a resident

Web URLs - Any website links containing resident-specific details

IP Addresses - Network identifiers used in digital communication

Biometric Identifiers - Fingerprints, voiceprints, retinal scans, etc.

Full-Face Photographic Images - Any recognizable facial images

Any Other Unique Identifying Number, Code, or Characteristic - Any information that could be uniquely linked to an individual

BEST PRACTICES

- ✓ Always verify authorization before sharing resident information.
- ✓ Use secure communication methods for transmitting PHI.
- ✓ Avoid discussing resident details in public or non-secure areas.
- ✓ Store physical and electronic records securely.
- ✓ Report any suspected privacy breaches immediately to your supervisor, compliance officer or privacy officer.

FSA
COMPLIANCE
COLLABORATIVE