HIPAA- 18 Identifiers of PHI and the 7 Elements of an Effective Compliance Program

By Frank Sivilli

The Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996 set forth industry standards on the handling of protected health information (PHI). PHI is an individually identifying health information classified by the Department of Health and Human Services (HHS) into 18 HIPAA identifiers.

The Department of Health and Human Services (HHS) lists the 18 HIPAA identifiers as follows:

1. Patient names
2. Geographical elements (such as a street address, city, county, or zip code)
3. Dates related to the health or identity of individuals (including birthdates, date of admission, date of discharge, date of death, or exact age of a patient older than 89)
4. Telephone 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
13. Device attributes or serial numbers
14. Digital identifiers, such as website URLs
15. IP addresses
16. Biometric elements, including finger, retinal, and voiceprints
17. Full face photographic images
18. Other identifying numbers or codes

While some of the 18 identifiers are straightforward, such as patient names and medical record numbers, others such as vehicle identifiers and IP addresses are surprising. Healthcare entities collect a wealth of information on their patients for various reasons, and all of the information they collect is protected under HIPAA.

A healthcare provider may collect a patient's vehicle identifier number (VIN) to issue a handicap pass or a copy of a driver's licenses as a means of identifying the patient. While seemingly innocuous, having a patient's VIN or Driver's license information, also provides an individual with malintent, the patient's home address, birthdate, what they look like, and for those with a handicap pass, their medical information. This information can be used for blackmail, or in extreme cases, to assume their identity. As such, many healthcare organizations that experience a breach are required to offer affected individuals free credit monitoring and identity theft protection.


18 HIPAA Identifiers
Below we've listed the 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services (HHS) Office of Civil Rights (OCR). HIPAA protected health information examples include:
1. Name
2. Address
3. Any dates
(except years) that are directly related to the individual
18
4. Telephone number
5. Fax number
6. Email address
7. Social security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Vehicle identifiers
ABC - 123
13. Device identifiers or serial numbers
14. Web URLS
https://www
IP
15. IP address
16. Biometric identifiers (fingerprints, voice prints, etc.)
17. Full-face photos
18. Any other unique identifying numbers, characteristics, or codes
AOA excel

The 7 Elements of an Effective Compliance Program

There is widespread confusion surrounding HIPAA compliance and what exactly it entails. As such, the HHS has released guidance on what makes up an effective HIPAA compliance program.

The HHS has identified 7 elements that make up an effective compliance program:

1. **Implementing written policies, procedures, and standards of conduct**

   Healthcare organizations are required to have written policies, procedures, and standards of conduct surrounding the handling of PHI. These must be customized to apply to the specific organization and their business processes.

2. **Designating a compliance officer and compliance committee**

   A compliance officer is an important aspect of any HIPAA compliance program. The compliance officer does not need to be a compliance expert, they do however need to be aware of the organization's compliance program. They also must be available for employees questions regarding the compliance program. In addition, a compliance committee should be established with members that advise the compliance officer on matters related to HIPAA compliance such as IT personnel, legal counsel, and privacy officials.

3. **Conducting effective training and education**

   Employees must be trained on an organization's policies and procedures, as well as HIPAA requirements. Training must be conducted annually, and documented to prove employees' attendance. The best way to conduct trackable training is through an online platform that can attribute certain actions to individual employees. This way healthcare organizations can be sure that all of their employees went through their complete training program.

4. **Developing effective lines of communication**

   One of the requirements of HIPAA is breach notification. This means, in the event of a breach, the breach must be reported in a timely fashion. Employees must be aware of who they should report suspected breaches to, and they must have a means to report breaches anonymously.

5. **Conducting internal monitoring and auditing**

   HIPAA law requires healthcare organizations to conduct six mandatory self-audits annually. The self-audits evaluate the organization's administrative, technical, and physical safeguards that are in place to secure PHI.

   - *Security Risk Assessment:* creates a standard device installation and setup process to be implemented across an organization.
   - *Privacy Assessment:* evaluates an organization's privacy policies to ensure that PHI is used and disclosed in accordance with HIPAA.

- *HITECH Subtitle D Audit:* ensures that an organization has proper documentation and protocols in relation to Breach Notification.
- *Security Standards Audit:* ensures that an organization's security policies are in line with HIPAA requirements.
- *Asset and Device Audit:* an itemized inventory of devices that contain ePHI. The device and asset list includes which employee(s) use the device and what security measures are in place securing the device.
- *Physical Site Audit:* each physical location must be assessed to determine if there are measures protecting PHI, such as locks or alarm systems.

The self-audits are meant to identify any gaps that may exist in security practices so that healthcare organizations can develop remediation plans to address those gaps.

6. **Enforcing standards through well-publicized disciplinary guidelines**

Healthcare organizations should have written policies and procedures to address internal healthcare breaches. An internal breach occurs when PHI is used or disclosed by an employee in an unauthorized manner. There should be clear, predetermined disciplinary actions for employees that do not uphold privacy standards.

7. **Responding promptly to detected offenses and undertaking corrective action**

Healthcare breaches must be reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) as well as affected individuals. Depending on the size of t the breach, reporting requirements differ.

- *Meaningful breaches:* are breaches affecting more than 500 individuals. Meaningful breaches must be reported within 60 days of discovery to HHS OCR, affected individuals, and the media.
- *Minor breaches:* are breaches affecting less than 500 individuals. Minor breaches must be reported by the end of the calendar year to HHS OCR and affected individuals.

An organization that experiences a healthcare breach must develop corrective action plans to ensure that a similar breach does not occur in the future. If the breach occurs from an internal entity, the organization should retrain employees to ensure that they understand what is permitted and what is not. Healthcare breaches that occur due to an external entity should assess security measures to determine where security gaps are. Once gaps are determined, remediation efforts should be implemented to address identified gaps.

In the event of a HIPAA audit, to be considered HIPAA compliant, it is not enough to have a compliance program, there must be documentation to prove HIPAA compliance efforts. Healthcare organizations that implement an effective compliance program will have the documentation necessary to prove their "good faith effort" towards HIPAA compliance.