Introduction and Disclaimer

This list is **not comprehensive**, it's intended to cover **only** the engineering and information technology aspects of the law. This checklist is intended as a precursor to prepare for a proper audit.

In no way is this document to be construed as legal advice or as a substitute for the actual text of HIPAA regulations.

Overview

- Safeguards for Protected Health Information
- The difference between protected and anonymous / aggregated data
- General rules on when each may be accessed
- Data that must be tracked

More Information / Consulting Services

Visit: www.scoutcorpsllc.com or www.hipaapotamus.com

Mail: info@scoutcorpsllc.com

HIPAAPOTAMUS
SCOUT CORPS

Safeguards for PHI

*This section applies to anything that contains **individually identifiable** heath information. Anonymous or aggregated information doesn't carry the same restrictions. (more detailed definitions appear later)*

*Everything on this list needs to be addressed **and documented**.*

Administrative Safeguards

1. Management Process
    - Risk Analysis
    - Risk Mitigation
    - Sanction Policy
    - IT System Activity Review
2. Assigned Security Responsibility
3. Workforce
    - Authorization and/or supervision
    - Clearance
    - Termination
4. Access Management
    - Isolation *(Ensure that information doesn't leak from the parts of an organization that have and use PHI to the parts that don't need to)*
    - Access Authorization
    - Access Modification
5. Security Training
    - Reminders
    - Protection from malicious software
    - Login Monitoring
    - Password Management
6. Incident Procedures
    - Response
    - Reporting
7. Contingency Plan
    - Data Backup Plan
    - Disaster Recovery Plan
    - Emergency Mode Operation
    - Testing and Revision (of the contingency plan)
    - Applications and data criticality analysis
8. Evaluation / Audit
9. Contracts with Associates and Subcontractors

Physical Safeguards

1. Access Controls
    a. Contingency Operations
    b. Security Plan
    c. Access Control and Validation
    d. Maintenance Records
2. Workstation Use
    a. Workstation Security
    b. Device and media controls
    c. Disposal
    d. Re-use
    e. Accountability
    f. Backup and storage

Technical Safeguards

1. Access Control
    a. Unique user identification
    b. Emergency access procedure
    c. Automatic logoff
    d. Encryption
2. Audit Controls
3. Integrity *(prevent improper deletion or modification)*
4. Authentication
5. Transmission Security
    a. Integrity
    b. Encryption

What it means to de-identify health data

Method 1 – Trust an Expert

"A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable".

Consider data in question alone, and/or in combination with other reasonably available information. Analysis must be documented.

Method 2 – Scrub the Data Clean of the Following

- Names
- Geographic subdivisions / location information more specific than a US state
  First 3 digits of the zip code is okay, if each combination of zip codes has >20,000 people
  Anyone/everyone in a smaller group of zip codes must be placed in 000
- Dates more specific than years
  - Birth, admission, discharge, death
  - Ages (or birthdates) 90 and above must be aggregated into a single "90+" category
  - Appointment and treatment dates
    Not specifically mentioned … it's probably best to chop out as much information as possible – for example, knowing that two treatments were 3 months apart without knowing ***which*** *months should suffice for a usage of data that's anonymous in the first place*
- Anything that's an identifier in another database somewhere
  - Phone numbers
  - Fax numbers
  - SSNs
  - Medical records numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle numbers
  - License plate numbers
  - Device identifiers
  - URLs
  - IP addresses
  - Biometrics (voice prints, fingerprints)
  - Photographs that include a full face
  - Anything that's ***like*** any of the above
- Remove any and all the above for
  - The individual
  - Their relatives
  - Household members
  - Employers

You *can* add your own internal ID to *re-identify* records, so long as…

- You don't use that ID for anything else (since that would allow someone to tie it back)
- It's not *derived* from any of the above fields (example: hash of name and SSN)

Who's Allowed to See …

For a *limited* data set (de-identified)

There must be an agreement in place covering:

- Who is the recipient of the data
- What the rules are on re-sharing the data
- What the recipient may do with the data
- Recipient is not permitted to attempt to re-identify the data
- Recipient will report breaches

Full data set with PHI

- Everyone who's accessing PHI must be HIPAA compliant
- Allowed circumstances
    - If shared *without* pre-authorization from the patient, only when
        - Necessary for the patient's care
        - Required by law
          Certain scenarios involving public health, disaster relief, etc.
    - If the patient is given an *opportunity to accept/refuse* (opt-out)
        - Family members
        - Directories (for hospital visitors to ask for you by name)
        - Members of the clergy
        - If the patient is incapacitated and is unable to express an accept/refuse preference, you may share information if (and only if)
            - It's consistent with prior expressed preference, or
            - It's in their best interests as assessed by the healthcare provider
    - Authorization from the patient *explicitly required* (opt-in)
        - Any opt-in must be informed and individually documented/provable
        - Anything not explicitly listed in the "opt-out" or "without pre-authorization" sections is assumed to be opt-in only
        - Examples (not comprehensive)
            - Psychotherapy notes (with exceptions for treatment and legal defense)
            - Marketing
            - Sales of data
            - Research studies

Must be Tracked

- Healthcare providers must be assigned NPIs (National Provider Identifier) by HHS; data providers must track those to identify providers for relevant transactions
- Standards and code sets are laid out for the following categories of interactions. These must be tracked in accordance with those:
  Note that this only applies to health care providers, not "clearinghouses" (aka data brokers)
  - Health problems – diseases, injuries, impairments, etc.
  - Actions – treatments, prevention, diagnosis, management, etc.
  - Drugs, etc.
  - Services – procedures, laboratory tests, ambulance transportation, etc.
  - Items – medical supplies, equipment, prosthetics, etc.
  - Encounters or transactions
  - Eligibility for an encounter or transaction
  - Referrals and certification
  - Claims and claim status
  - Enrollment and disenrollment
  - Funds transfers and remittance advice
  - Premium payments transactions
  - Coordination of benefits transactions
  - Medicaid pharmacy "subrogation" (substitution) transactions