HIPAA Factsheet - From privacy.globe1234.com

HIPAA regulates release of personal health data from health providers, health insurers and clearinghouses.

Exempt Recipients

HIPAA allows release (without patient authorization) for:

Medical staff	Family & friends when relevant to their involvement or payments
Investigators	People at risk of communicable disease
Auditors	Public health agencies (including foreign)
Inspectors	Social services agency to help victims of abuse
Licensing bureaus	Discovery requests (e.g. divorce)
Organ banks	Emergency preparedness (NYTimes story)
Coroners	Military commanders (about service members)
Medical examiners	Prisons (about prisoners)
Funeral directors	Police and any other law enforcement
Secret Service	Researchers on anonymous data, or onsite, or on the dead, or locally approved
Targets of threats	Workers' compensation purposes
Spies	Food and drug businesses approved by FDA (to monitor side effects)
Subpoena	Employer for "medical surveillance *of the workplace and work-related illnesses" if* employer
Summons	requested any care

All medical records can be **subpoenaed**, as explained by ABA. Electronic records are cheaper to subpoena than paper records, since copying is cheaper.

Federal rules of evidence do **not** protect doctor-patient confidentiality in federal courts, though most state courts do.

Disclosures have the same limits for 50 years after death.

Identifiers

HIPAA also **allows release** if the following are *removed*: patient/ relatives/employer names, ID numbers, addresses (except state or 3-digit zip with 20,000+ people), IP addresses, URLs, equipment numbers, month and day of any event, birth years 90+ years ago must be combined, biometric IDs (e.g. finger/voice prints), "full-face photographs and any comparable images, Any other unique identifying number, characteristic, or code," such as dental charts, DNA, unique scars and tattoos.

This list allows releases with your age, doctor names, and diagnoses by year, which data brokers can compare to your social media postings. Movers can be identified by comparing a series of 3-digit zip codes to public voter registration records.

Exempt Providers

HIPAA **does not cover** the following:

- online and offline stores (know health items you bought)
- credit card companies
- social networks (know your messages about your and your friends' health)
- life insurers
- employers
- workers compensation carriers
- most schools and school districts
- many state agencies like child protective service agencies
- most law enforcement agencies
- many municipal offices
- health care providers small enough that they don't electronically send health insurance claims and eligibility to insurance companies

Frequent Breaches

From 2003-2013, medical records were released improperly in 116,000 incidents. Most affected 1-499 people, and these incidents are not listed publicly.

From 2003-2012 federal enforcers investigated 18,559 of the cases of noncompliance that people complained about, and resolved these cases "by requiring covered entities to take corrective actions and/or provided technical assistance to covered entities to resolve indications of noncompliance" (p.7). They had money penalties in up to 21 cases, totaling $25 million.

The federal government lists 1,000 incidents. In each of these incidents 500 to 5 million medical records were released improperly, totaling 31,300,000 people, 5% paper and 95% electronic. Most were breached by stealing a computer or smart phone with **un**encrypted patient records. A record fine, $4.8 million, was for accidental internet release of 6,800 patients' records ($700 fine/patient). The federal site does not yet include cases which are still under investigation, such as 80 million records taken from Anthem, announced in February 2015.

Electronic Medical Records

The policy drive for electronic records makes it easier to breach privacy on large numbers of records, by accident or by theft. Federal standards for electronic systems do not protect privacy.

An extensive article in Politico says hackers can sell medical records for hundreds of dollars, and people use them to get prescription drugs for resale. An article in Wired says companies with big business outside health care, like Google (and Kimberly Clark) are leaving the business of health care to avoid liability when things go wrong

The government rarely imposes penalties for privacy breaches, and it is hard for individuals to sue for damages, though they may claim deceptive privacy statements, or other grounds.

No Privacy Online or Shopping

Patients' web browsing, purchases and social media comments are not secret and often reveal their diseases. A good poster and study show how hundreds of data brokers buy this health information and spread it widely.

Data brokers comb releases to see the names which use each IP address, and keep those names on file. Thus in homes with a fixed IP address, no browsing is anonymous. At businesses where many users share IP addresses, the brokers can't always identify people, but they can track the web use of the business overall, and thus its plans. Top executives or departments may have distinctive browsers (e.g. presence or absence of cookies, use of certain websites), so they would stand out from the company as a whole.

A longer explanation of medical privacy is at the Privacy Rights Clearinghouse.