patientprivacyrights

Final Omnibus Privacy Rule: Summary from the Patient Perspective

By Deborah C. Peel, MD

The Omnibus Privacy Rule is not a “privacy” rule. It's actually a “security” rule. Under the law, the word “privacy” means an individual's right to control the collection, use, and disclosure of personal information. But neither Congress nor HHS has adopted a definition of the word "privacy," so concepts of privacy and security are unclear, confused, and conflated. The data protections described in the final rule are security protections (a term HHS has defined), not privacy protections. However, the fact remains that the public does not support “meaningful use” of their data without “meaningful consent” that allows them to control when, where, how, and by whom their data are used.

HITECH was designed to "promote widespread adoption and Interoperability of health IT." HHS has "general authority” to increase workability and flexibility, decrease burdens on industry, and better harmonize the Privacy Rule with other HHS regulations. But HHS has not “harmonized” the regulations with other strong state and federal laws, citizens’ Constitutional rights to health information privacy, or the AMA Code of Medical Ethics. Promoting systems that ensure patient control over sensitive personal information for routine use is does not appear to be a priority for HHS. Given the void at the federal level**,** some states have passed laws that are stronger than HIPAA to better protect patient data from misuse and harms, such as banning data sales and re-identification. Clearly, states should now take the lead and guide the nation back to data protection frameworks that enable citizens to trust electronic health systems.

Strong New Protections for Patients

- HIPAA/HITECH are affirmed as the "floor" for data protection. States can require greater privacy and security protections.
    - HIPAA only supersedes "contrary" state laws.
- Business Associates (BAs) and subcontractors are required to comply with all provisions.
    - Data security protections and standards apply to all "downstream" entities.
    - HIOs, PSOs, e-RX gateways, PHRs, RLSs, governance entities, data storage companies, shredding companies, and all others that hold or transfer data are BAs.
    - An entity is a BA if it meets the regulatory definition of BA, regardless of whether it has a contract with a covered entity (CE) or not.
    - Disclosures of PHI for "management and administration" do not create a BA relationship.
    - If a BA makes disclosures that are not required by law, it must obtain "assurances" the PHI will be kept "confidential."
    - BAs are liable for civil penalties.
- Adds key new data security protections.
    - Security requirements and risk assessments are required.
- Adds new enforcement and increases penalties for some violations.
    - AGs can enforce HIPAA/HITECH (this was added because OCR failed for years to enforce violations).

    - Increased fines (fines were too low). The new $1.5M maximum fine per calendar year is still too low to be more than a slap on the wrist for many corporations, but it's better than $25K/year.
        - Regarding breach: multiple requirements can be violated and each is counted separately. For example, impermissible use or disclosure and safeguards violations have separate penalties, so total penalties can exceed $1.5M.
    - Requires the Secretary to investigate and impose civil penalties for "willful neglect."
    - The Secretary's ability to impose civil penalties is barred only if criminal penalties are imposed.
    - The Secretary "may" proceed directly to formal enforcement without exhausting information resolution efforts in cases of "willful neglect."
    - OCR will determine "willful neglect" and proceed in every case even if "willful neglect" was not found at preliminary review.
- Patients have enforceable rights to obtain copies of PHI maintained in one or more designated records sets.
    - Right of access exists regardless of the format of PHI within 30 days.
    - If not readily reproducible, then in an agreed upon format.
    - Patients may direct CE to transmit copy to designee.
    - Fee must not be greater than labor cost, reasonable cost-based fees are allowed.
    - CEs may require request for copies in writing, not the same as an authorization, which contains many more elements.
    - Images or other data linked to the data sets must be included.
    - CEs must verify identity.
- Providers are fully liable for disclosures if they accept cash and agree to restrictions.
- Parents can give oral or informal agreement for CE to disclose immunization records to schools, eliminating the requirement for parental authorization.

Weak Patient Protections

- Most marketing uses of PHI now require authorization, but 2 of 3 exceptions limit effectiveness:
    - Promotion of adherence to current medications or biologics, for refills and generic alternatives, and for related equipment such as insulin pumps—patients should give informed consent for these marketing contacts.
    - Promotion of health in general, but no specific products or services—patients should give informed consent for these marketing contacts.
- New enforcement provisions lessen or eliminate penalties for breaches in many or most cases.
    - If entities quickly correct security flaws they may not be penalized.
    - The Secretary has discretion about applying penalties for violations.
    - HHS can seek resolution without penalties for every violation except "willful neglect."
- Patients who pay out-of-pocket for treatment or medication (or someone else can pay for them) were supposed to be able to prevent disclosure of PHI to health plans. However, the rule does not ensure PHI will not be disclosed.
    - The rule advises that paying cash and using a paper prescription will cause pharmacies to keep paper prescription records private by not digitalizing or selling them, but that won't happen. Pharmacies will simply type prescription information into electronic systems; they will not maintain paper prescription records systems in addition to electronic systems.

- Pharmacies are not required to comply with requests to restrict disclosures, so all prescriptions can be reported to health plans even if you pay cash.
- HHS does not require segmentation technologies so that PHI can be protected and selectively shared. Instead the information is "flagged" so only the "minimum necessary" information is disclosed; HHS assumes CEs routinely comply with requirement to disclose only the “minimum necessary” information but there is no proof that CEs comply.
- HHS appears to believe that segmentation of data must be done manually, as if robust segmentation technologies do not exist and are not in wide use.
- HHS states that patients are responsible for notifying and preventing "downstream" providers from disclosing of PHI to health plans, i.e., the protections do NOT flow electronically. "downstream" with the data. This suggests that technology to protect data downstream does not exist, which is not the case.
- If a provider is able to "unbundle" services in a bill, the provider ***should*** do so in order to restrict disclosure of PHI paid for out-of-pocket. This appears to mean that providers can decide whether any services a patient pays for out-of-pocket will be disclosed or not.
- CEs must disclose PHI paid for out-of-pocket for Medicare and Medicaid audits as required by federal law. This provision ensures that Medicare beneficiaries receive the same quality of care as other patients, but weakens protections for data security and privacy of all other patients.
- If a Medicare beneficiary refuses to authorize submission of the bill to Medicare for service, the provider must restrict the disclosure of PHI to Medicare.
- Cash payments are also prohibited for patients on Medicare and/or Medicaid, which appears to eliminate their rights to keep any information private and contradicts the provision above.
- HMO patients paying cash must use out-of-network providers to restrict disclosures of PHI, only if not prohibited by contract or state law.
- Health plans can disclose restricted PHI to coordinate benefits with another plan.

- Telecoms with "random access" to PHI are not BAs.
- Data transmitters without "routine access" to PHI are not BAs.
- "Small Provider" loophole:
  - Can hire a company to de-identify data without a BA agreement because it "lacks the expertise to provide instructions."
- GINA's requirements intended to protect genetic data are unenforceable and confusing.
  - There is no requirement for auditing or verification to ensure health plans and insurers comply with regulations.
  - Genetic information cannot be used for "underwriting" by health plans, with the single exception of issuers of long-term care policies, regardless of when or where the information originated.
  - An authorization cannot be used to allow the use of genetic information for underwriting by health plan.
  - GINA states nothing limits health plans from increasing premiums for “manifested” diseases, but 'manifested' diseases cannot then be used as genetic information about other individuals and used to increase their premiums.
  - GINA prohibits group health plans, health insurers, and Medigap issuers from collecting genetic information or requesting or requiring individuals undergo genetic testing.

        - The Final Omnibus Rule prohibits insurers from using or disclosing genetic information for underwriting, but there is no way to prevent insurers from viewing genetic information/PHI already in EHRs.
    - Prohibits employers from requiring, requesting, or purchasing genetic information and strictly limits disclosures.
        - However, there is no way to prevent employers from viewing genetic information/PHI already in EHRs.
- Fundraising use and exposure of very detailed PHI than proposed in the NPRM is now allowed without authorization.
    - CEs may disclose demographic info, including names, dates of birth, gender, addresses, contact information, dates of hospitalization, department of service, treating physician, and patient outcomes (e.g., death and sub-optimal treatment outcomes), for fundraising.
    - CE is expected to disclose only the minimum necessary to BAs, and BAs must also first screen the PHI before use.
    - Patients may not opt-out before receiving the first fundraising communication.
    - The NPP must include notice of PHI use for fundraising.
    - **Requirements don't protect patients and instead facilitate hidden surveillance, data mining, and sales of PHI inside and outside the healthcare system.**
- Enforcement of the Final Omnibus Privacy Rule depends primarily on whether contracts between entities are enforced. Contracts do not enforce themselves any more than laws do. Therefore, most enforcement of the rule depends on inside whistleblowers.
- The Security Rule is "scalable" to different sizes of CEs and BAs and depends on their "resources," which means smaller and poorer entities will have weaker, less expensive data security protections. However patients won't know that their data may be in systems with weaker protections.
- Meaningful, frequent external auditing of processes, technologies, and compliance with the rule is not required.
- Research access to PHI without meaningful, informed consent is greatly expanded.
    - The public does not support research access to PHI.[1] Only 1% would agree to unfettered access to PHI for research.
    - Consent must still be on paper. There is no requirement to use interactive, robust electronic consent technologies.
        - Electronic consent/authorization could eliminate the need for IRB and Privacy Board approval of research using PHI.
    - "Compound Authorizations" are now allowed, except involving psychotherapy notes
    - Authorization for combined clinical trials and biobanks are allowed.
    - Allows authorizations for all future research, replacing consent that is study-specific; allows future secondary use of data.
    - All research and public health use of PHI is allowed without meaningful patient consent/authorization.

[1] Alan Westin's Survey and Study for the IOM on how the HIPAA Privacy Rule Affects Research: http://patientprivacyrights.org/media/WestinIOMSrvyRept.pdf?docID=2501

        - Health-related corporations are becoming research institutions, as PPR has been pointing out for years, because claiming to use/purchase data for “research” or “public health” enables access and use without patient consent.
            - EHRs, insurers, PBMs, pharmaceutical vendors, HIT vendors, business analytics companies, and marketing companies are all doing “research” and “public health.”
        - An entity (such as an IRB) that reviews, approves, and provides research oversight is not a BA.
- Sale of PHI for marketing requires patient authorization, but the exceptions are so numerous it's hard to think of instances where authorization is required.
    - A product or service in the health plan can be marketed without authorization.
    - “Enhancements" that "add value" to a plan can be marketed.
    - Communications about "treatment, case management, and care coordination" can be marketed.
    - Communications about a drug or biologic currently prescribed can be marketed as long as the payment is "reasonable."
    - Marketing mammography equipment to a patient would not require authorization if sent by a charity organization.
    - A CE may receive non-financial or in-kind donations of materials to distribute to patients without authorization, such as materials describing a health product or service.

Major Loopholes for Use of PHI the Public Does/Will Not Agree With

- ***There is no entity (such as a CE or the patient) that has a list of all subcontractors of a BA***
    - ***This means there is no transparency or accountability for PHI downstream, despite HHS' intent to ensure that data protections "do not lapse."***
    - ***Hidden flows of data destroy trust in HIT and physicians.***
- 50 years after death, our health data will be open for all uses; we cannot prevent this exposure.
- 3rd party recipients of PHI are exempt from the regulations.
- Freestanding PHRs not attached to EHRs are exempt from regulations.
- After a death, PHI may be disclosed to family members or others involved with care unless the decedent prohibits disclosures.
    - Why does the default mode result in exposure of PHI to family and friends rather than a presumption of the decedent’s wish for privacy?
    - This allows CEs to decide whom to disclose PHI to based on their "involvement."
- Banks are not required to comply with HIPAA, despite having PHI (names of your doctors and hospitals written on checks; names of medications on credit card charges).
- Banks can share medical records the same way they share credit information (Gramm-Leach -Bliley Financial services act).
- Credit bureaus can use/receive PHI (stipulated in many NPPs).
- Many key violations are not easily discoverable or enforceable.
    - No “chain of custody” for PHI, no right of consent for routine disclosures, no data map for hidden flows of health information. Therefore, there is no transparency or accountability for use and disclosure of PHI.
    - No way to know if data are re-identified.

- Many key security and privacy violations can only be found via whistleblowers.

- Rules perpetuate the fantasy that data de-identification works
  - Page 300: HHS believe that it would be "very difficult to re-identify limited data set that excludes dates of birth and zip codes."
- Violates Congress' intent that *all* breaches be reported to HHS.
  - If PHI is encrypted, no breach notice is required.
  - The Secretary is to be notified of breaches of more than 500 records no later than 60 days following discovery. Breaches of lesser numbers of records are reported and kept in a log 6 years.
  - Congress explored and then specifically rejected a "harm standard" –it felt patients had a right to know about all breaches PHI, which indicates the level of data security protections provided by the CE or BA.
  - An "impermissible use or disclosure is presumed to be a breach" unless the CE or BA demonstrates "low probability that data has been compromised."
  - HHS "believes a bright line standard would be extremely burdensome and costly for entities to implement."
  - The NPRM required a "harm" standard before breach notice, so if there was little chance of financial, reputational, or other harm to an individual, the breach did not need to be reported.
  - The final rule replaces the "harm" standard with a "risk assessment" about the probability that data was compromised. If the breached entity decides the probability is "low," it does not need to report the breach—the decision about risk to the patient is made the breaching entity.
  - HHS identified the basic elements of a risk assessment but does not require an independent organization to assess risk.
  - The final rule empowers breached entities decide about whether breaches present risks or cause harms to patients; surely this puts CEs and BAs in major conflicts of interest. Again there is no meaningful, required, regular external oversight or auditing of CEs and BAs.
  - HHS allows CEs and BAs to determine likelihood of re-identification, when it is well known in computer science that re-identification is very easy using multiple available public data sets.
- Notice of Privacy Practices (NPP)
  - Even though the Omnibus Privacy Rule is the "floor" for privacy, the Rule does not require an explanation of how patients can exercise their rights to control PHI under stronger state laws, common law, tort law, federal laws other than HIPAA such as 42 CFR Part 2 and 7332, or their Constitutional rights to privacy and health information privacy.
  - The NPP is not required to list all situations requiring authorization, but where else is the patient supposed to find out?
  - The NPP is not required to describe record-keeping of psychotherapy notes, even though some CEs, by policy, prohibit requiring consent for the disclosure of psychotherapy notes or blend the psychotherapy notes into the general medical record, eliminating the protections in HIPAA/HITECH.
  - Inclusion of rights if PHI is breached must be included, as well as the right to restrict disclosures if you pay out-of-pocket for treatment.