The remedies matrix: a framework for assessing remedies

Applied Example: Health Insurance Portability and Accountability Act (HIPAA)

What are the highest-level policy goals of the regime?

Policy goals

=> To protect people from losing their health insurance when they change or lose a job; to standardize healthcare information to increase efficiency and protect patients from the disclosing of their personal health information (PHI); to standardize the amount of savings available from a pre-tax medical savings account; to set guidelines for group health plans; to prohibit the use of tax-deductions on life insurance plans, company endowments, and company contracts

Deterrence: How does the regime seek to deter bad behavior? Options may include direct punishment (fines), redress of harms (compensation), denial of benefits (disgorgement of profits or other benefits), and cost imposition (e.g., a tax or fee).

Direct punishment, such as fines paid to the government

=> The penalty for HIPAA Violations can be assessed by either DHS's Office of Civil Rights (OCR) or State Attorney Generals. These penalties have four tiers for civil charges which have increasing monetary values and three tiers for criminal charges which have increasing monetary values and prison sentencing

Redress remedies to individuals (which may include restitution or other money damages)

=> HIPAA does not officially establish a method of individual restitution but under certain state laws individuals may be able to sue for negligence or breach of contract when they can prove damages or injuries allowing them to gain a class or individual restitution

Denial of benefits (such as disgorgement of profits or data deletion)

=> HIPAA does not provide for denial of benefits

Cost imposition (including taxes or fees)

=> HIPAA does not include systematic and intentional cost imposition

Does the regime include a mechanism to hold the bad actors' assets at risk?

=> HIPAA does not include a mechanism to hold bad actors assets at risk

Does the regime contemplate the problem of over-deterrence?

=> HIPAA places a ceiling on the maximum fine able to be assessed for each tier of HIPAA violation to help prevent overdeterrence

Is there a market for noncompliance?

=> Yes, in the case of intentional non-compliance this generally occurs when companies do not reveal a data breach to protect their reputation or illegally sell health data. These both pose greater penalties than for unintentional noncompliance. Nonetheless neither of these are particularly common and noncompliance with PHI by entities who do not fall under HIPAA is much more common

Are attorney fees available to successful plaintiffs?
=> HIPAA does not allow for the recovery of attorney fees

How does the regime seek to compel good behavior (carrots or sticks)?
Preapprovals (permits, licenses)
=> None

Injunctive relief
=> If awarded by courts

Safe harbors
=> There are multiple safe harbors from liability for violations of HIPAA. De-identified data loses the restrictions on use and disclosure and thus covered entities are not liable for sharing this. Further, mitigating factors or affirmative defenses such as the harm caused and ability to pay are considered when assessing penalties for HIPAA violations and can reduce charges. Leniency is also given when industry-standard security measures are shown with the addition of the recently passed HIPAA Safe Harbor Bill which

Role of Gatekeepers and Third Parties
Does the ecosystem for the sector/practice include gatekeepers (e.g., third party service providers) who regulate conduct?
=> There are two types of third-parties under HIPAA. The first is “business associates” who transmit PHI or offer a personal health record for a covered entity or are a subcontractor that interacts with PHI on behalf of a business associate. The second type of third-party is entities that have a role in collecting PHI but are not covered under HIPAA and have no relationship with the original covered entity.

How does the regime address third parties who are involved in the underlying unwanted behavior?
=> Business associates are responsible for the same HIPAA regulations as their covered entities who can be found liable for violations of their business associates and thus covered entities are recommended to ensure their third-parties maintain adequate security and follow HIPAA regulations. If a third-party collects PHI from a covered entity with the patient's authorization but is not covered by HIPAA, this data is no longer protected by HIPAA and neither is liable for it. However, if the third-party was created or operates on behalf of the covered entity then the covered entity is still liable for HIPAA violations arising from this data.

Other Issues
How does the regime address the problem of guile?
=> Compliance reviews can be instituted to ensure that covered entities are following HIPAA; The complaint process allows individuals to bring HIPAA violations to the attention of the DHS.

How does the regime address collective wrongs (small injuries to many people)?
=> Technically HIPAA does not provide a private right of action for individuals to sue, requiring DHS’s Office of Civil Rights and State Attorney Generals to enforce HIPAA. However, in recent years individuals have begun class action lawsuits under certain state laws for HIPAA violations specifically when injuries or damages can be proven due to negligence or breach of a contract.

How does the regime address power differentials among victims and wrongdoers?
=> State Attorney General enforcement; DHS complaint process; State class action

How does the regime respond to technological change?
=> DHS has the authority to pass rules that help the regime stay up to date with technological changes. These include additions in the past two decades such as HITECH, the Breach Notification Rule, and the Final Omnibus Rule that have all contributed to keeping HIPAA rules up to date in areas such as encryptions, mobile devices, and breaches. Ultimately this has only limited success as rules are often slow to match technology and HIPAA still only covers certain entities.

Regulatory Structures

Is the regime complemented by an agency and what are that agency's powers?
=> The DHS's OCR is the primary enforcement arm of HIPAA through which it investigates complaints, conducts compliance reviews, and does education and outreach work. The investigative phase generally ends with voluntary compliance, corrective action, or resolution agreements but if these are not resolved, civil penalties can be instituted. If criminal violations are believed to have occured the investigation may be referred to the Department of Justice

Monitoring or investigation?
=> Primarily investigation, however some corrective action plans the DHS OCR makes with companies do require monitoring to ensure compliance with the settlement.

Overall Assessment of Efficacy

Does the regime achieve desired policy outcomes?
=> Overall HIPAA has succeeded in its goals of standardizing certain administrative and tax areas and establishing a baseline for the privacy of PHI. However, it's lack of flexibility and speed in addressing the rapid advancement of technology and the sharing of personal information has somewhat weakened it. Numerous third-parties are not bound by HIPAA due to the specifics of its language and the larger surveillance economy as a whole has made many of its provisions fundamentally moot as PHI becomes broadly available due to this weakness. Ultimately, HIPAA succeeds in establishing a privacy baseline and as an administrative standardization method but needs to become more adaptable to help fully protect PHI