HIPAA Privacy Compliance and Enforcement

2019 ABA Section of Taxation May Meeting

Kim Wilcoxon
Overview

- HHS Enforcement
- Private Lawsuits
  - Under ERISA
  - Under state law
- Additional HIPAA Issues
  - HIPAA transactions Compliance Review Program
  - Alexa becomes HIPAA-compliant
As of February 28, 2019, OCR has settled or imposed a civil money penalty in 63 cases resulting in a total dollar amount of $99,581,582.00.

Source: [https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html](https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html)
HHS has identified the following compliance issues as the ones investigated most often (in order of frequency):

- Impermissible uses and disclosures of protected health information
- Lack of safeguards of protected health information
- Lack of patient access to their protected health information
- Lack of administrative safeguards of electronic protected health information
- Use or disclosure of more than the minimum necessary protected health information
HHS has identified the following common types of covered entities that have been required to take corrective action to achieve voluntary compliance (in order of frequency):

- General Hospitals
- Private Practices and Physicians
- Outpatient Facilities
- Pharmacies
- Health Plans (group health plans and health insurance issuers)
HHS conducted a pilot audit program to identify best practices, identify risks, and encourage compliance

- Phase 1 (2011-2012) – onsite audits of 115 covered entities
- Phase 2 (2017-2018) – desk audits of 166 covered entities and 41 business associates

Compliance found with breach notifications and privacy notice requirements

Most room for improvement found with risk management and risk analysis
HIPAA does not provide a private right of action

Lawsuits could be brought under ERISA

- The HIPAA privacy and security rules require that certain HIPAA compliance provisions be included in health plan documents

- ERISA §502(a)(2): The DOL, a participant, or a beneficiary may sue for breach of fiduciary duty for failure to follow the terms of the plan

- ERISA §502(a)(3): A participant or beneficiary may sue for appropriate equitable relief to enforce the terms of the plan

- The insurer of an employer’s health plan allegedly mailed information to a participant in an envelope with a large window.
- The participant’s health information, including HIV status, was visible through the window.

ERISA Section 514 preempts state-law claims that relate to employee benefit plans.

The disclosure at issue was made by the TPA of the employer-provided health plan in which the plaintiff was enrolled.

BUT, the court found that the claims related to the TPA’s mishandling of sensitive health information.

The fact that Plaintiff was a participant in an employer-sponsored plan had no import.
State Law Claims and ERISA Preemption

  
  - ERISA Section 502 preempts state-law claims if
    
    - Plaintiff, at some point in time, could have brought the claim under ERISA Section 502(a)(1)(B) and
    
    - There is no other independent legal duty implicated by the defendant's actions
State Law Claims and ERISA Preemption

  - The following claims were preempted because Plaintiff did not allege an independent legal duty that was not based on the ERISA plan documents
    - Breach of contract
    - Negligence
    - Negligent infliction of emotional distress
  - A claim for invasion of privacy was not preempted because it was based on an independent duty under state law
State Law Claims and ERISA Preemption

- Quintana v. Lightner, 818 F.Supp.2d 964 (N.D. Texas 2011)
  - Plaintiff was a participant in an employer-provided health plan
  - Plaintiff was injured in an automobile accident
  - The health plan’s subrogation subcontractor disclosed the plaintiff’s health information to the liability carrier for the party that allegedly caused the accident
  - Plaintiff sued for invasion of privacy
Quintana v. Lightner, 818 F.Supp.2d 964 (N.D. Texas 2011)

- The court found that the invasion of privacy claim was not preempted under ERISA Section 502
  - Plaintiff was not alleging a violation of the terms of the plan or attempting to recover benefits under the plan
  - Plaintiff was asserting an independent right to privacy
- The court noted that the plan could have included a waiver term in the subrogation section of the SPD, but that it was silent on disclosure
  - Accordingly, the vendor exceeded the scope of its authority under the plan and its conduct was not protected by ERISA

- Former employee and spouse contacted the employer's HR director to discuss whether they were covered by the employer’s health plan.

- The HR director allegedly repeatedly requested information about their medical conditions, but they refused to provide it.

- The spouse later disclosed the information to the plan’s insurer.

- The HR director allegedly manipulated an employee of the insurer to obtain the information.

- The HR director allegedly publicized their medical information with the intent of embarrassing and discrediting the employee.

- Three state law claims were filed against the insurer
  - Breach of fiduciary duty not to reveal confidential information
  - Negligence
  - Violation of a state medical information confidentiality statute

- The court held that, because the information was sought and disseminated for inappropriate reasons, the claims did not have a connection to an employee benefit plan and therefore were not preempted by ERISA

- Disclosure was not made in the course of providing benefits or performing duties under an ERISA plan.
(Unpublished opinion from Court of Appeal of California, Fifth Appellate District)

- Plaintiff was diagnosed with liver failure and was issued a nurse case manager by the TPA of her employer’s health plan.

- At the nurse case manager’s request, Plaintiff signed an authorization form.

- The nurse case manager allegedly disclosed Plaintiff’s increased need for a liver transplant to the employer/plan sponsor/plan administrator pursuant to the authorization.

- Plaintiff’s employment was terminated, allegedly shortly after the disclosure.

- Plaintiff’s claim file was allegedly closed following termination of employment and was allegedly reopened at the employer’s request following Plaintiff’s initiation of wrongful termination lawsuit.
State Law Claims and ERISA Preemption

  
  *(Unpublished opinion from Court of Appeal of California, Fifth Appellate District)*

- Plaintiff sued for invasion of privacy and unfair business practices, premised on the TPA’s alleged improper disclosure or use of Plaintiff’s personal health information.

- The court found that both claims were preempted by ERISA.

  - The complaint implied that the employer terminated Plaintiff’s employment following receipt of Plaintiff’s medical information but did not allege that the TPA improperly disclosed information for the purpose of having Plaintiff’s employment terminated.

  - The complaint did not allege conduct outside of the scope of plan administration.

- Case management services were covered by the plan.

- The TPA’s evidence indicated the plan administrator needed access to the information in order to monitor plan expenditures, benefit utilization and potential large claims.
(Unpublished opinion from Court of Appeal of California, Fifth Appellate District)

We conclude that, when, as in this case, a plaintiff asserts state law claims based on alleged misconduct that was within the scope of the conduct regulated by ERISA, including the privacy protections required to be included in ERISA group health plans, invoking state law remedies for that alleged misconduct constitutes an impermissible attempt to enforce ERISA privacy rights by means of an alternative enforcement mechanism; as to those claims, the state law provisions have an impermissible connection with ERISA plans and are therefore preempted.

In other HIPAA News . . .
The CMS Division of National Standards announced the Compliance Review Program to ensure compliance among covered entities with HIPAA Administrative Simplification rules for electronic health care transactions.

- HHS will randomly select 5 health plans and 4 clearinghouses in April 2019
- Not limited to those who work with Medicare or Medicaid
A voluntary pilot program evaluated compliance of 4 clearinghouses and 1 health plan

- All but 1 underwent a corrective action plan as a result of the program

Types of violations discovered during the program:

- Transactions (42)
- Code Sets (15)
- Unique Identifiers (14)
- Operating Rules (3)
HHS makes initial contact with randomly selected entity.

HHS works with initial contact to identify the best point(s) of contact at the entity for the Compliance Review program.

HHS furnishes entity with a packet describing how to participate, information needed, and available resources.

HHS’s Compliance Review contractor provides instruction on accessing the EIDM portal and uploading files for the entity.

After this instruction has been provided, the entity has 30 days to submit transactions and other artifacts to HHS.
HHS reviews artifacts within 30 days of receipt.

HHS provides findings to entity.

HHS specifies any necessary corrective action.

If corrective action is not needed, the compliance review is concluded, and the entity is notified.

When any corrective action is required and completed, HHS validates compliance.
Prep Steps for health plan sponsors

- Ask TPA to verify that they are handling electronic transactions in a compliant way.
- Confirm that the services agreement with the TPA requires compliance with HIPAA Administrative Simplification rules for electronic transactions.
Amazon has announced software that allows Alexa to securely transmit medical information

Six voice programs have been announced, including:

- Cigna’s voice program allows employees of large national clients to manage health improvement goals and earn wellness incentives
- Express Scripts’ voice program allows participants to check the status of home delivery prescriptions