

Privacy-State v. Federal Issues

INTRODUCTION

While Congress labeled some efforts at medical privacy *simplifying* it may have been *tongue in cheek*. What has resulted from HIPAA and its regulations is a clash of federal and state rules on practices that will take years of struggle and clarification to resolve.

- State rules on medical privacy are many and varied, disjointed and confusing, complex and inconsistently enforced.
- HIPAA rules on privacy added a new layer of laws, some of which preempt the state laws and some of which do not.
- One group of health plan players (insurers, the Blues and the HMOs) will abide by one of rules; another group (plans and their sponsors) will abide by another. The insured v. self-funded *playing field* will eventually experience a new *tilt*.

HIPAA RULES

The HIPAA privacy rules, further clarified by the HHS Regulations, represent the first effort to put in place a nationwide set of medical privacy standards.

What was a free flow of information is now only history. Compliance with the new requirements will be long, painful and expensive. The penalties are of such severity that few will be casual in compliance.

All of the health care plan players are affected in that the *covered entity* definition is very broad:

- Providers
- Clearinghouses
- Health plans
- Plan supervisors
- Most plan vendors
- Business partners of above.

HIPAA defines the limits within which Protected Health Information (medical vendors primarily) may be freely exchanged. Outside the limits, patient authorization is needed. Coverage may not be conditioned on such authorization being accepted by the patient.

Where medical treatment is concerned, HIPAA does not place any restrictions on the free flow of medical information. In other circumstances only the minimum amount of medical data shall be.

STATE PRIVACY LAWS

The states, individually and collectively, have a plethora of disjointed hodge-podge of privacy laws and regulation. A few states have up to 40 or 50 separate laws on medical privacy.

- Most of the states ban the use of PHI without some type of patient authorization by providers and insurers (including HMOs).
- Most states have rules relative PHI obtained by state agencies (insurance departments, e.g.).
- Only rarely is there a state privacy law that affects an employer.
- Many of the state privacy laws are disease-specific (AIDS, mental disorders, substance abuse, e.g.) where a stigma is attached to the condition.
- Waiver of privacy laws is found where public health considerations are more important than privacy (rabies, e.g.).
- Many state laws deal with special situations (court proceedings, medical research, e.g.).
- States affix fines and penalties for breaches of medical privacy.
- States typically permit access of the patient to such patient's own medical records. Access includes getting a copy thereof.

A few states have a medical privacy law of the comprehensive type. The experience of the states that did enact the comprehensive model was not favorable. These were numerous *unintended consequences* that are not discussed herein. It is reported that states are preparing to adopt their own privacy law patterned after the Federal models; Texas is one such state.

ERISA PLAN CONSIDERATIONS

The burden is on the employer, as an ERISA plan sponsor, to (a) see that PHI is identified (b) amend plan documents and (c) modify any rules and protocols to achieve compliance.

ERISA plans are in three classes:

1. **Fully Insured (Insurer, Blues or HMO)**
The employer has no risk and does not receive only medical privacy information. The privacy laws do not apply to such employer.
2. **Hybrid Plans (Self-Funded, However Administered)**
The privacy law applies to the employer in such arrangements whether the administration is by the employer, a TPA or an insurer.
3. **MEWAs and VEBAs**
The privacy rules apply to these arrangements but not to the sponsoring employers, if any.

Of great significance is the laws' prohibition against medical information being used by the employer for employment-relation actions. A wall of protection between plan data that is *protected* and *non-protected* is essential.

As a *relief valve* for workers' compensation, ERISA provides that it shall apply except where necessary to comply with workers' compensation laws.

Gramm-Leach-Bliley (GLB)

Privacy-State v. Federal Issues

- 2 -

The Financial Services Modernization Act of 1999 (the GLB law) requires that financial institutions (insurers, e.g.) must limit disclosure of *nonpublic protected health information* (PHI). States are mandated to promulgate regulations to accomplish this restriction.

The NAIC Model Regulation called Privacy of Consumer Financial and Health Information Model Regulation meets the GLB mandate. The NAIC model provides that meeting HIPAA privacy standards equates to meeting the GLB mandate.

FEDERAL STATUTE PREEMPTION

In General

The application of the preemption principle is difficult; the only safe and practical approach is that each state privacy law must be appraised against HIPAA and the preemption issue settled on a law-by-law basis. This could, and likely will, take years to do.

ERISA Preemption

This principle established by the many years of ERISA litigation will doubtless serve as the guide in determining HIPAA preemption. The likely expectation is that insured plans would have to meet the more demanding of state privacy law or HIPAA. The self-funder would only need to meet the demands of HIPAA.

HIPAA Preemption

HIPAA specifically provides that contrary state laws are superseded. There are a number of state laws that are saved from preemption:

- Public health related (child abuse, disease monitoring, e.g.)
- Where auditing, evaluation or licensure is involved.
- Where anti-fraud considerations exist
- Where insurance regulation is concerned
- Where controlled substances are involved
- Where studies relative health care delivery or the costs thereof are involved
- Other compelling public welfare considerations exist.

HHS is loathe to offer any opinions relative to HIPAA-state law preemption because the expected volume would be so great.

Certain principles to be followed are offered; a state will be deemed preempted if (by way of examples):

- It is not contrary to HIPAA.
- It is contrary but not stringent.
- It provides a public health service.

- It serves a perfunctory, regulatory, auditing or licensing purpose.
- It has an anti-fraud purpose.