The Evolution of Medical Privacy Regulation

Strong Standards For 21st Century Health Care

Donna A. Boswell

March 7, 2008

HOGAN & HARTSON

HIPAA: a good acronym

HOGAN & HARTSON

- Today, we are talking about the federal medical privacy regulations promulgated under the HIPAA statute--
  - Not the new fraud and abuse requirements
  - Not the new health insurance portability requirements
  - Not the new standards for electronic health administrative transitions

HIPAA: A Strong Foundation

HOGAN & HARTSON

- Some, who may not understand how HIPAA's complex requirements work in practice, have been led to fear that it does not protect confidentiality.
- In reality, HIPAA is more protective of patient privacy than many states' laws or standard medical practices pre-HIPAA.
- ***NOTE: An important disconnect stems from the fact that quality care in the 21st century depends on communications and information much more than it did in the era of the sole practitioner.***

HOGAN & HARTSON

HIPAA In Its Historical Context (OR) How Did We Get Here?

"In The Beginning…"

HOGAN & HARTSON

- Medical privacy was not really a state or federal statutory phenomenon; it emanated from medical ethics and the doctor's oath—
  - "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about."
- ***NOTE: Nothing in the HIPAA privacy regulation changes the applicability or requirements of this oath or professional codes of ethics.***

Standard Practice pre-HIPAA…

HOGAN & HARTSON

- At the initial visit, obtain a consent to treatment, including consent to obtain, use and disclose medical information for treatment and third party payment, if any.
- When other parties request information – lawyers, employers, life insurers, police – ask them to produce the patient's written consent, or a court order, subpoena, etc.
- Some providers, particularly those working in socially sensitive areas, stopped obtaining the "blanket" consent and required their own specific patient consent for each disclosure, even when the request is from another doctor treating the patient.
- ***NOTE: Nothing in HIPAA changes these practices EXCEPT where HIPAA is MORE protective of privacy.***

What are the state laws?

HOGAN & HARTSON

- Some states have codified the practice of permitting a broad general consent or waiver into law, regulation, accreditation, licensure, state contracting and/or rules of evidence for state court.
- And some states codified specific requirements for handling one or more of the following types of information: drug abuse, sexual abuse, child abuse, mental health, HIV, STD, genetics.
- ***NOTE: Nothing in HIPAA changes these laws EXCEPT where HIPAA is MORE protective of patient privacy.***

What is the problem for interoperable clinical records?

HOGAN & HARTSON

- Multiple, inconsistent requirements even within a single state --
  - State laws governing pharmacies, labs, physicians, nurses, physical therapists, hospitals and health plans are almost never the same.
  - States have different laws for different types of information – such as different forms of consent for HIV information than for genetic information, etc.
- ***NOTE: The HIPAA preemption standard says that ALL applicable state AND federal laws must be complied with unless it is IMPOSSIBLE to comply with both AND the state law is less protective of medical privacy.***

Interoperable health records--

HOGAN & HARTSON

- Based on all of the available evidence, interoperable health records offer our best option for improving the quality of care and the efficiency of care in the 21st century.
- High quality care using 21st century facilities and interventions cannot be delivered without access to coherent, accurate, and complete information about the patient's history, diagnostics, and concomitant current treatment.
- ***NOTE: Laws to protect privacy while enabling care that meets current standards of quality should be our primary objective.***

In 1996, Congress authorized the HIPAA privacy regulations

HOGAN & HARTSON

- HIPAA's administrative simplification requirements facilitate EDI for certain administrative and financial transactions between health care providers and payers.
- Congress failed to reach agreement on what the uniform federal medical privacy standard should be, but recognized that
  - These interstate transactions necessitate a federal standard, and
  - some state laws were less protective of medical privacy than necessary in the EDI context.

Congress' HIPAA privacy requirements…

HOGAN & HARTSON

- Instructed HHS to consult with the National Committee on Vital and Health Statistics and the Attorney General in developing recommendations regarding—
  1. "The rights that an individual who is a subject of individually identifiable health information should have."
  2. "The procedures that should be established for the exercise of such rights."
  3. "The uses and disclosures of such information that should be authorized or required."

And Congress provided …

HOGAN & HARTSON

- A deadline to ensure that medical privacy regulations addressing the areas set forth in the HIPAA statute would be implemented before any of the other transaction standards; and
- Federal civil and criminal penalties would be applicable to individuals who violate the medical privacy regulations.
- Congress separately required the Secretary to establish uniform federal *security* standards for electronic health information, and these standards were intended to preempt state laws.

HIPAA Final Regulation…

HOGAN & HARTSON

- Addressed all of the matters required by statute
- Established rights based on the privacy principles generally recognized in international circles:
  - Right to access and copy medical information
  - Right to notice of information practices (i.e., uses and disclosures to be made on a routine basis in providing health care and health benefits)
  - Choice to avoid data collection by an entity whose routine practices are unacceptable and to prohibit non-routine disclosures to third parties by refusing to sign an authorization
  - Assurances regarding the security standards in place to protect the information from use or disclosure by third parties and by inappropriate employees and contractors.

1999

HIPAA Timeline…

HOGAN & HARTSON

- Bundled consent prohibited. Secretary Shalala published proposed regulation in March 1999.
  - It proposed to prohibit providers from obtaining a general consent or waiver for the use and disclosure of information as a condition of treatment.
  - Instead, patients would be given detailed notice of privacy practices involved in routine health care uses of patient information, and
  - The regulation required that specific written authorization be obtained for non-health care disclosures.
- Routine Medical Use Limited. The Secretary was clear that she believed this proposal was consistent with current medical practices with respect to routine use of patient information for treatment, payment and certain limited administrative activities of the provider or payer currently treating or providing benefits to the patent, but more protective by fully informing the patient and providing an opportunity to object.

2000

HIPAA Timeline, continued…

HOGAN & HARTSON

- Some public comments objected that the Secretary had failed to require specific consent for each health care disclosure as a matter of federal law
- So Secretary Shalala modified the final rule on December 28, 2000, to make prior specific consent mandatory for providers who have "direct" treatment relationships" with the patient.
- Secretary Shalala established exceptions to the consent requirement for direct providers—
  - In an emergency,
  - Or if the provider has an obligation to treat the patient,
  - Or if language or other barriers make it difficult to obtain consent..
  - So long as the provider documented that the requirements of one of the exceptions was met.
- Other new HIPAA protections remained in place.

2002

Added complexity plus HIPAA penalties…

HOGAN & HARTSON

- Physicians, pharmacies hospitals and patients decried to the un-workability of this new consent requirement and incompatibility with medical practice.
- On August 14, 2002, Secretary Thompson amended the final rule essentially to go back to the initial proposal Secretary Shalala had published, making doctors and other direct providers subject to the same prohibitions on non-routine use and disclosure as others in the health care system.
- Made the obtaining of specific consent for routine health care uses optional for direct treatment providers, consistent with Secretary Shalala's proposal.

2003 Effective date forward

Today's result…

HOGAN & HARTSON

- The HIPAA regulation's provisions are more generally protective of patient privacy than the routine consent/waiver practices in place under state law, regulations, licensure and contracting requirements, and rules of legal evidence.
  - For example, HIPAA prohibits a provider (or a health plan) from obtaining a routine consent or authorization for non-health care uses and disclosure as a condition receiving treatment.
  - State laws requiring specific written consent for each treatment disclosure of HIV, spousal abuse, child abuse, genetic or psychiatric information remain in place *and* augment the HIPAA authorization requirements for non-routine disclosures.

Since HIPAA's 2003 Effective Date…

HOGAN & HARTSON

- **Authorization Required Except for Routine Uses.**
  - Medical information may not be used or disclosed for other than the patient's health care or health benefits, and the administrative activities of the entity treating or providing benefits, without a patient's written authorization.
- **Notice of Routine Uses Required.**
  - All patients have the right to notice of the routine health care uses of their medical information made by providers and payers and providers must obtain the patient's acknowledgement of receipt of this notice
- **Right To Request Greater Restrictions on Use.**
  - All patients must be informed that they have the right to ask that their specific consent be obtained before such routine uses, and to know their provider's response before electing to obtain care from that provider.
- **Treatment May Not Be Conditioned on Authorization.**
  - Authorization for medical records to be used for other purposes must be independent of the patient's treatment or payment or administrative purposes of that health care provider
  - No more blanket authorizations for provider or health plan use or disclosure of medical records for research.

And HIPAA requires…

HOGAN & HARTSON

- No routine employer access to medical claims
  - Self-insured employers that pay claims directly must establish firewalls and are subject to criminal penalties for accessing or using patient information for other than health plan benefits.
- Doctors, labs, hospitals and health plans that are not currently treating or insuring an individual cannot have access to his or her medical information without the patient's written authorization.
- Psychiatric notes cannot be disclosed for any purpose or to any person without the patient's specific authorization.
- Disclosures to journalists are limited; disclosures to friends not involved in patient care are limited.
- Use of patient information for provider fundraising is limited.

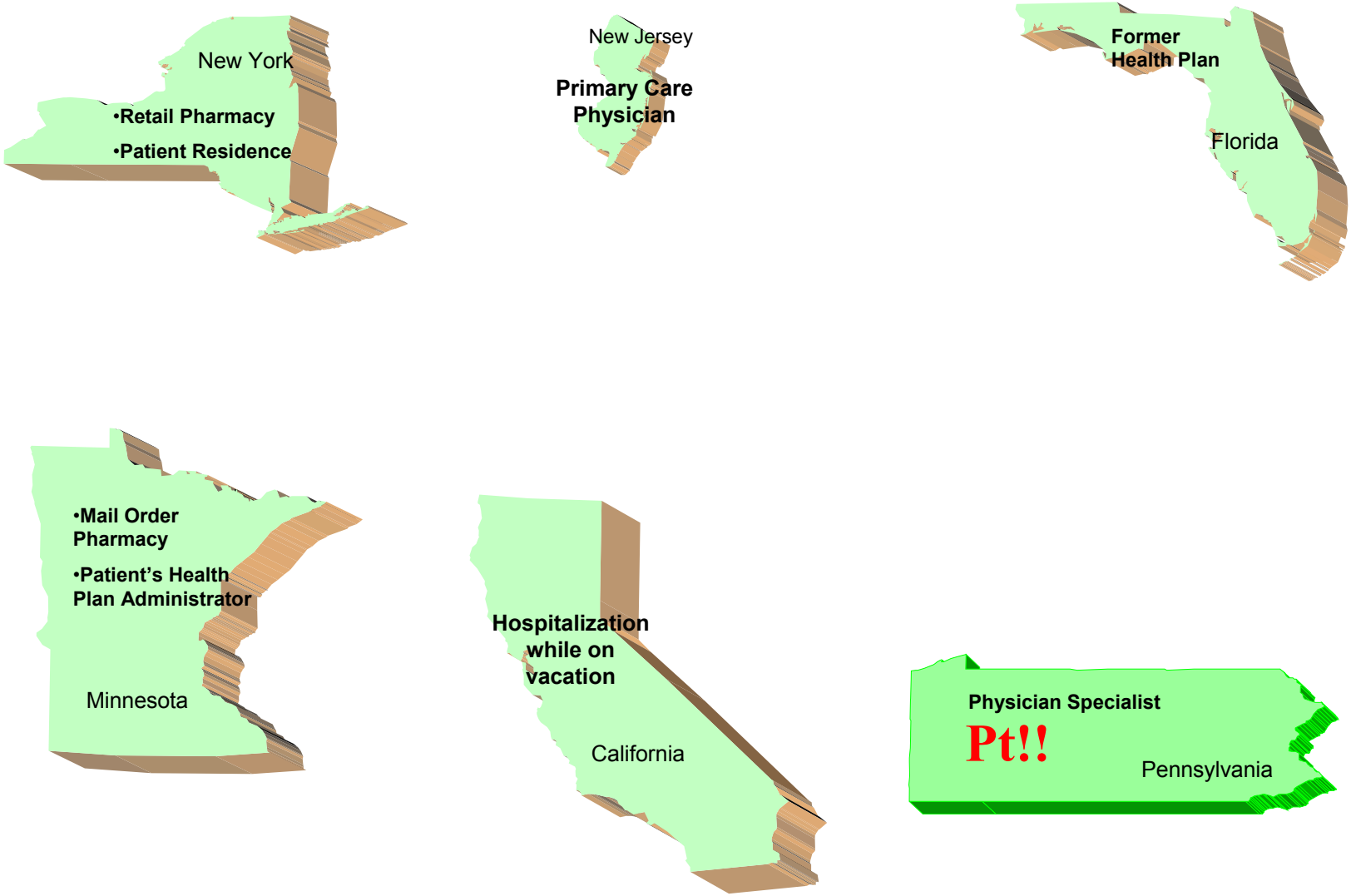
And HIPAA Requires…

HOGAN & HARTSON

- Contractors ("business associates") are obliged to limit use and disclosure of information to those activities for which they were lawfully hired and to provide security.
- Researchers, including providers who conduct research, cannot use identifiable medical records for research without the patient's authorization or waiver by an IRB in accord with protective federal criteria.
- Strict standards for "de-identification" of data sets before third parties are permitted to use or analyze it.
- Governments, including the US government, cannot access medical information without a law permitting such access, or the patient's authorization.
- All patients have a right to see and copy their medical records.
- Patients may request an accounting of the disclosures of medical information for other than their treatment, benefits and routine administration.

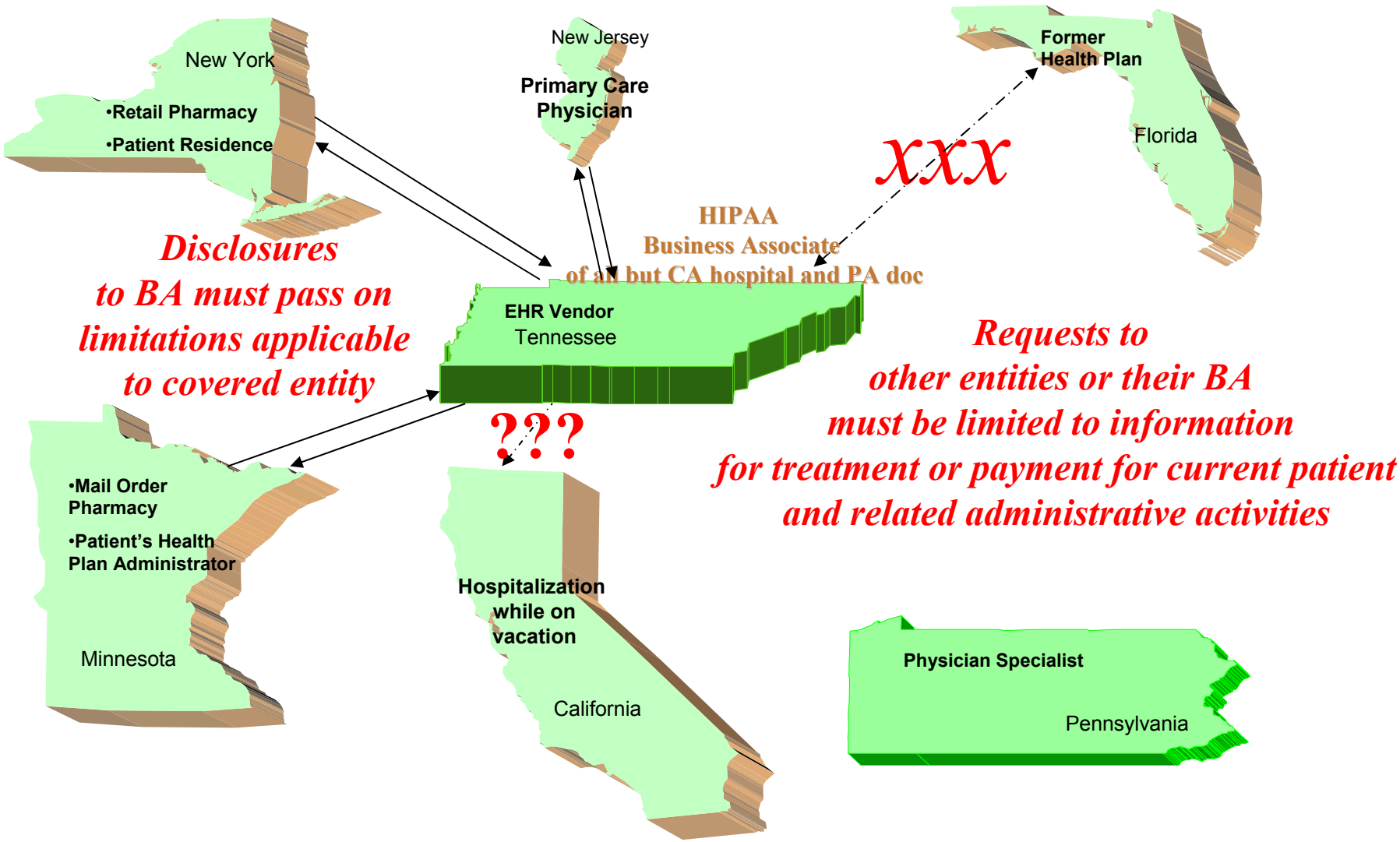
One patient's 21st century health care...

HOGAN & HARTSON



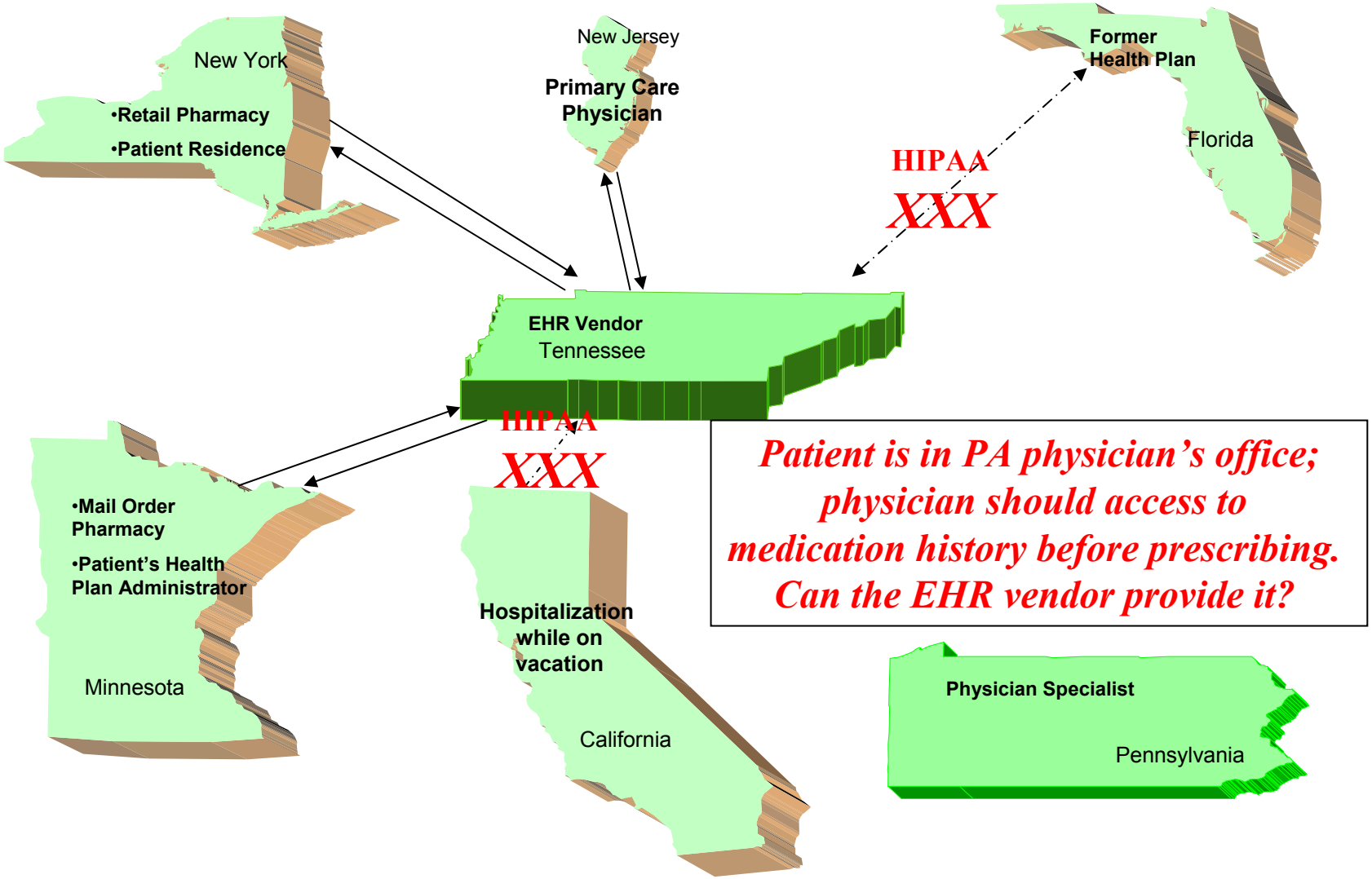
The EHR World under HIPAA…

HOGAN & HARTSON



Add in state law…

HOGAN & HARTSON



Legal Issues affecting the answer…

HOGAN & HARTSON

- Each provider and/or health plan must comply with the applicable state laws of its jurisdiction.
- HIPAA prohibits any of them from authorizing a business associate to make any use or disclosure of information that it could not do itself.
  - Assume that no Tennessee law applies to the EHR vendor directly
  - But the vendor has access to patient information in NY, NJ and MN only because it is a HIPAA business associate of an entity that is subject to specific state laws.
- *It is not consistent with HIPAA for a provider or health plan to participate in an EHR system where its HIPAA BA will be disregarding state laws that apply to the provider.*

Policy Issues …

HOGAN & HARTSON

- It is not feasible to require the vendor to require to comply with all laws applicable to doctors, hospitals, pharmacies, labs, physician assistants, nurses, health plans in all of the states where it has business associates:
  - The laws are not consistent;
  - The laws have not anticipated the complexity of modern health care and health benefits;
  - The laws change.
- Providers likely will not participate in EHR projects if they will be responsible for state law issues with respect to the vendor.
- The improvements in quality of care that are being sought through EHR cannot be achieved if providers cannot access relevant medical history.
- *It is a waste of effort and money to build a system that no one can use without legal ambiguity and risk.*

Consumer Interests…

HOGAN & HARTSON

- I want to know what standard applies to protect information about me and I don't want it to depend on who has the information
- I don't want to have to get a lawyer to tell me what law applies because my information has been lawfully transmitted across state lines
- I don't want to have to remember tell the names of all my drugs, doctors or immunizations and dates of last screening for various conditions – I want EHR
- I don't want to have to remember and fill out forms on which of my relatives have had what conditions – I want EHR
- *I want to be confident that my providers and health plans to have access to the basic information needed to provide the services I have requested; I am not competent to know precisely what that is, but I know that there are some things I want to be kept secret.*

If we want an interoperable EHR…

HOGAN & HARTSON

- State laws will no longer be able provide differing protections.
  - The paperwork requirements for providers to comply with state laws that apply to them will make it untenable to participate in an interoperable EHR:
    - Either some form of overbroad consent will be given as Secretary Shalala reported in publishing the original rule
    - Or if consent is not given, information will be blocked from further access and in some cases, will make the EHR too costly for the value given
- Consumers will be even more confused about what rights they have (and what they have signed away) and may well refuse to obtain treatment from physicians that participate in an EHR unless we can provide uniformity of protection.

Next steps…

HOGAN & HARTSON

- HIPAA can provide the starting framework but --
  - Who is accountable for compliance, for example, with respect to security, authentication/blocking of system users, and breach issues; how can we create more uniformity of protection?
  - What information should be routinely accessible (e.g., psychiatric notes are not) to providers?
  - How can we implement the existing requirement that providers have a current relationship with the patient in order to access information held by others
  - Do we need additional protections, such as distinguishing ability of a provider to *access* information from the ability to *download* and make further use and disclosure of the information?

HOGAN & HARTSON

For more information on
Hogan & Hartson, please visit us at

www.hhlaw.com

Baltimore
Beijing
Berlin
Boulder
Brussels
Caracas
Colorado Springs
Denver
Geneva
Hong Kong
London
Los Angeles
Miami
Moscow
Munich
New York
Northern Virginia
Paris
Shanghai
Tokyo
Warsaw
Washington, DC