Vermont H. 121

Introduction

Chair Marcotte, Vice Chair Jerome, Ranking Member Nicoll (pronounced Ni-cole), and members of the committe. Thank you so much for the opportunity to speak with you today.

My name is Christina Glabas I am the owner and founder of Gazelle Consulting, a HIPAA compliance and data privacy consulting firm that serves organizations nationwide and internationally. I had the honor of working with the Oregon DOJ to develop Oregon's Consumer Privacy Act, which passed in July of this year. And have now been asked to assist clients who are being audited under this law, which has given me a pretty interesting full circle perspective on the topic of the boundary of healthcare data in the law.

I've worked with over 100 different businesses, from social workers to software conglomerates, to help them develop privacy and security programs ranging from HIPAA to GDPR to CCPA. So I've seen first hand the challenges and successes that businesses have in adapting to the demanding pace of technology growth and what I have learned, is that businesses do not understand the technology that they've built. There is a critical role that regulators must play in this moment, and that is to give businesses enough practical guidance to make meaningful impacts on protecting consumers privacy so businesses can get back to doing what their good at.

Data compliance is the cost of doing business in this era

Their real jobs aren't cyber security specialists, but until their business model stops depending on data, they are going to have to learn to how to be ethical stewards of it. Right now, our society and its technology functions on a data ecosystems, and that means until the government can take some of this out of the hands of every business, we'll need to find way to help businesses protect the surprisingly precious information they may have about any and all consumer. If we as a society, don't provide guidance and resources on HOW to keep up with the threats and issues in managing data, companies won't bother doing it because they don't know how.

I understand firsthand the need for this legislation to be workable, and affordable, feasible. We've leaned on great legislation from GDPR and CCPA to guide the specificity in this bill and learned from businesses that had to comply with them as well in the past 10 years.

Yes, managing your data is challenging, but it's the cost of doing business in this era. But there is a big benefit of doing this work for companies, which is that they don't fall behind in protecting their systems from data loss, lack of maintenance, or technical debt.

Data privacy laws contain the groundwork for inventorying one's data and the information systems that contain them and how they use the data. It's quite difficult to explain just how critical this is for businesses who ALWAYS encounter unknown unknowns when assessing their systems using data privacy frameworks.

Exempting HIPAA

I am in full support of Vermont's Consumer Privacy bill, particularly because it includes an limits entity level exemptions related to HIPAA.

In order to ensure that this bill does not conflict with HIPAA or inhibit the provision of care, HIPAA data created by covered entities and their business associates are exempt.

Requests have been made for an entity level exemption for these businesses, which offer services both related and unrelated to healthcare, most obviously pharmacies within retail stores, or online conglomerates selling retail and health related services.

The bill has struck a compromise between consumers and businesses by not allowing an entity level exemption for businesses who are ALSO HIPAA Business Associates, unless the data is indistinguishable from and treated in the same manner as HIPAA data.

While I wholeheartedly support this bill, I urge the state of Vermont to oppose any further entity level exemptions, especially those related to HIPAA. Being a Business Associate under HIPAA does not obligate organizations to administer privacy rights under HIPAA, as they are only required to comply with the data security provisions of HIPAA, like encryption and access control. Only a Covered Entity may grant patients access to their data. Broadening entity level exemptions to include businesses with *some* healthcare contracts would leave a void of access to privacy rights for consumers who have no Covered Entity in the chain of custody who must ensure their privacy rights.

HIPAA Limitations

HHS Definitions

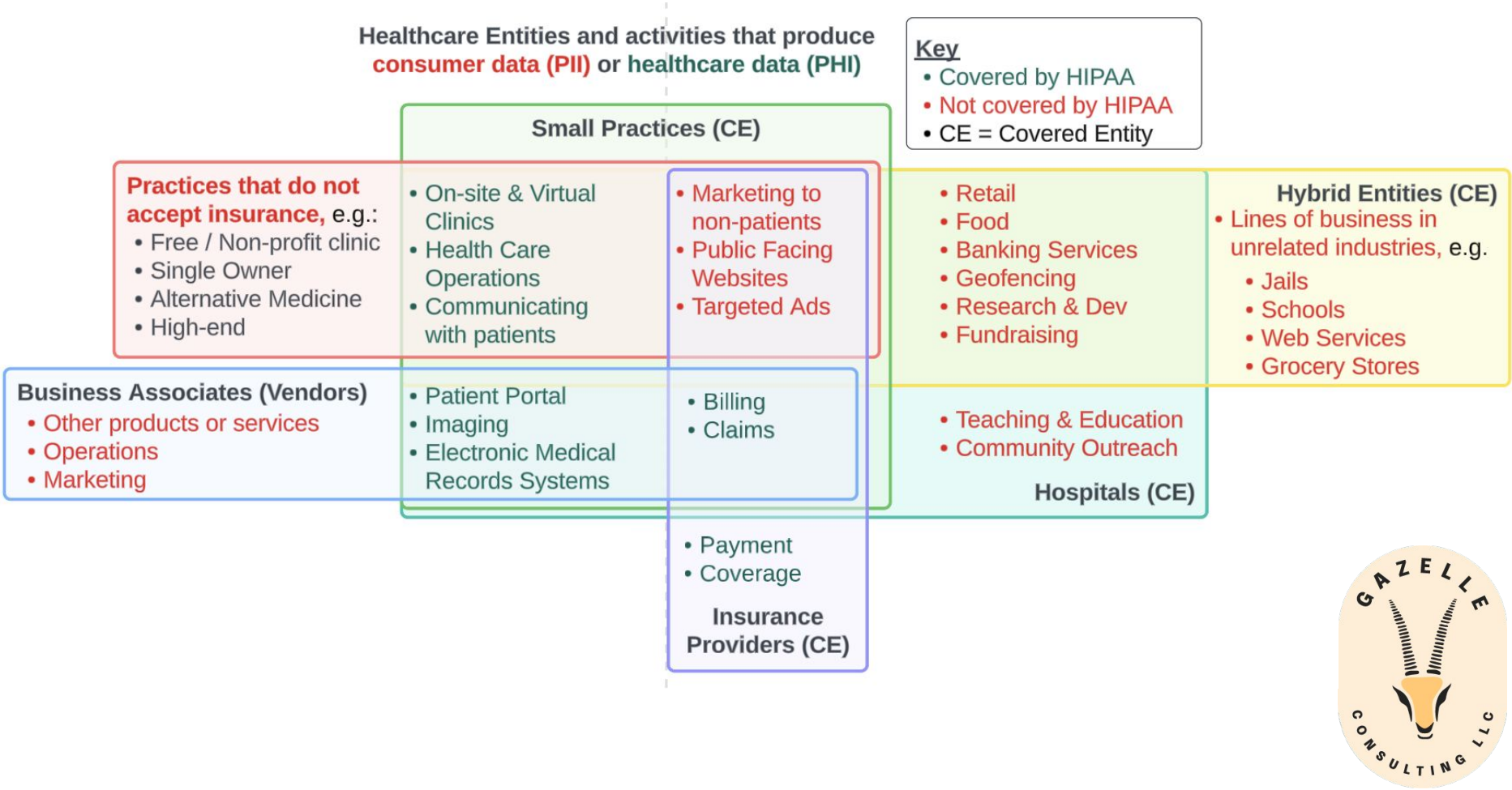
1. **Covered Entity**
    a. A health plan. An individual or group plan that provides, or pays the cost of, medical care. Health plans include private entities (e.g., health insurers and managed care organizations) and government organizations (e.g., Medicaid, Medicare, and the Veterans Health Administration)
    b. A health care provider. A provider of health care services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. **Health care providers (e.g., physicians, hospitals, and clinics) are covered entities if they transmit health information in electronic form in connection with a transaction for which a HIPAA standard has been adopted by HHS. (e.g., billing)**
    c. A health care clearinghouse. A public or private entity, including a billing service, repricing company, or community health information system, that processes non-standard data or transactions received from another entity into standard transactions or data elements, or vice versa.

2. **Business Associate**

A person or entity **that performs certain functions or activities** that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

A Covered Entity is one of the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.


Healthcare Entities and activities that produce consumer data (PII) or healthcare data (PHI)
Key
• Covered by HIPAA
• Not covered by HIPAA
• CE = Covered Entity
Small Practices (CE)
Practices that do not accept insurance, e.g.:
• Free / Non-profit clinic
• Single Owner
• Alternative Medicine
• High-end
• On-site & Virtual Clinics
• Health Care Operations
• Communicating with patients
• Marketing to non-patients
• Public Facing Websites
• Targeted Ads
• Retail
• Food
• Banking Services
• Geofencing
• Research & Dev
• Fundraising
Hybrid Entities (CE)
• Lines of business in unrelated industries, e.g.
• Jails
• Schools
• Web Services
• Grocery Stores
Business Associates (Vendors)
• Other products or services
• Operations
• Marketing
• Patient Portal
• Imaging
• Electronic Medical Records Systems
• Billing
• Claims
• Teaching & Education
• Community Outreach
Hospitals (CE)
• Payment
• Coverage
Insurance Providers (CE)

Close Out

It has been a true honor to testify in support of this bill. I believe this bill is absolutely necessary to protect citizens of Vermont by addressing gaps in HIPAA and providing recourse for harms.

Representative Priestly, their team at the DOJ, and the team that they have assembled to contribute to this bill is an impressive representation of consumer advocates, privacy specialists, and major technology companies.

I believe this bill will go far in protecting the citizens of Vermont and allowing businesses the flexibility to use the data to support their operations in an ethical way.

Thank you!