KILLING HIPAA

. . . It's About Time

This Program Offers 1.0 Hour of MCLE Participatory Credit

STATE BAR OF CALIFORNIA | BUSINESS LAW SECTION

DATE: **May 4, 2017**

TIME: **12:00 pm – 1:00 pm**

PRESENTERS: **Craig B. Garner, Esq.**
Grant B. Gelberg, Esq.

Garner Health Law CORPORATION

HYSM
HUANG YBARRA SINGER & MAY LLP

INTRODUCTION

All things truly wicked start from an innocence.

-- Ernest Hemingway

The Hippocratic 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." (1943, Translation from Greek by Ludwig Edelstein)

- "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know. Most especially must I tread with care in matters of life and death." (1964, Louis Lasagna, Academic Dean of the School of Medicine at Tufts University)

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Glossary

- Administrative Simplification: Gives federal agency mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of PHI.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

more Glossary

- Business Associate: Generally an entity or person who performs a function involving the use or disclosure of PHI on behalf of a CE (such as claims processing, case management, utilization review, quality assurance, billing) or provides services for a CE that require the disclosure of PHI (such as legal, actuarial, accounting, accreditation).
- Covered Entity (CE): An entity that is subject to HIPAA.
- Data Use Agreement: An agreement between a CE (the holder of the PHI) and the recipient of the PHI (such as a research investigator) in which the CE discloses a limited data set for purposes of research, public health or health care operations.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

more Glossary

- Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside of the entity holding the information.
- DOJ: The United States Department of Justice Department of Justice.
- Electronic Health Record (EHR)/Electronic Medical Record (EMR): An electronic record of health-related information on an Individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.
- Electronic Protected Health Information (ePHI): PHI in electronic form.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

more Glossary

- Health and Human Services (HHS): The federal government department that has overall responsibility for implementing HIPAA.
- Health Information Technology for Economic and Clinical Health Act (HITECH): Pub. L. 111-5.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA): Pub. L. 104-191.
- Hybrid Entity: A CE whose covered functions are not its primary functions.
- Individual: The person who is the subject of PHI.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

more Glossary

- Minimum Necessary: Refers to reasonable efforts made to limit use, disclosure, or requests for PHI to the minimum necessary to accomplish the intended purpose.
- Office of Civil Rights (OCR): The agency of HHS that is responsible for administering and enforcing HIPAA's privacy, security and breach notification rules.
- Protected Health Information (PHI): Any individually identifiable health information, including genetic information and demographic information, collected from an Individual, whether oral or recorded in any form or medium that is created or received by a CE.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Circa 1996

- WebTV is introduced.
- Sony enters the PC market with the release of its VAIO.
- Google is first developed.
- www.myspace.com goes live.
- Apple stock hits a 10-year low of less than $18.00/share.
- First version of Java is released.
- The price of gasoline is $1.22.
- The U.S. postage Stamp is 32 cents.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Stupidity has a knack of getting its way.

-- Albert Camus

HIPAA (Public Law 104–191)

- To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.
- Within 18 months of enactment, the Secretary of HHS is required to adopt standards from among those already approved by private standards developing organizations for certain electronic health transactions, including claims, enrollment, eligibility, payment, and coordination of benefits. These standards also must address the security of electronic health information systems.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Protections Under HIPAA

- In direct opposition to the fundamental tenet for which it now stands, the introduction of HIPAA did not originally include privacy legislation, but was modified in November 1999 to address patient concerns.
- Some 52,000 public comments and another year later, HHS issued final regulations known as the HIPAA Privacy Rule.
- HHS again modified the Privacy Rule in March 2002, and after 11,000 more public comments, issued its directive in August 2002.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Protections under HIPAA continued

- HIPAA's Security Rule governing "e-PHI" (2003)
- Enforcement Rule (2006)
- Breach Notification Rule as well as HITECH (the Health Information Technology for Economic and Clinical Health Act) Enforcement Rule (2009)
- Updated Administrative Simplification Rule (2013)

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA – Privacy

Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit . . . recommendations on standards with respect to the privacy of individually identifiable health information.

- The rights that an individual who is a subject of individually identifiable health information should have.
- The procedures that should be established for the exercise of such rights.
- The uses and disclosures of such information that should be authorized or required.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA – Penalties for Failure to Comply

- Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
- A penalty may not be imposed if it is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that such person violated the provision.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA – Penalties for Failure to Comply continued

A penalty may not be imposed if–

- The failure to comply was due to reasonable cause and not to willful neglect; and
- The failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA – Penalties for Failure to Comply continued

A person who knowingly and in violation of this part–

- Uses or causes to be used a unique health identifier;
- Obtains individually identifiable health information relating to an individual; or
- Discloses individually identifiable health information to another person;
- Shall be fined not more than $50,000, imprisoned not more than 1 year, or both.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA – Penalties for Failure to Comply continued

- If the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
- If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA AND MENTAL HEALTH

When the prison doors are opened, the real dragon will fly out.

-- Ho Chi Minh

HIPAA – Preemption

Federal law preempts state law, except when the state law:

- Is necessary to prevent fraud and abuse, ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery or costs or for other purposes.
- Addresses controlled substances.
- Relates to the privacy of individually identifiable health information.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Exception – Psychotherapy Notes

- Section 164.510(b)(3) of the HIPAA Privacy Rule permits a health care provider, when a patient is not present or is unable to agree or object to a disclosure due to incapacity or emergency circumstances, to determine whether disclosing a patient's information to the patient's family, friends, or other persons is in the best interests of the patient.
- Federal law refers to psychotherapy notes as excluded from access (45 CFR Section 164.524).
- But California does not set aside psychotherapy notes. California law wants to provide access to such health care records by patients.
- There are limits to this disclosure, however (Health and Safety Code Section 123115 (b)).

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Exception – Psychotherapy Notes continued

- Providers should make a determination if there would be a "substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records requested by the patient."
- Make a written record, to be included with the mental health records requested, noting the dates of the request and explaining provider's refusal to permit inspection or copying.
- Include a description of the specific adverse or detrimental consequences to the patient that the provider anticipate.
- Permit inspection by, or provide copies of the mental health records to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor, designated by request of the patient.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Exception – Psychotherapy Notes continued

- Inform the patient of the refusal to permit the inspection or obtain copies of the requested records, AND
- Inform the patient of the right to require the provider to permit inspection by, or provide copies to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or licensed professional clinical counselor designated by written authorization of the patient.
- Indicate in the mental health records of the patient whether the request was made as set forth above.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA and EMTALA

- A health care provider's "duty to warn" generally is derived by standards of ethical conduct and state laws/court decisions.
- HIPAA permits a provider to notify a patient's family members of a serious and imminent threat to the health and safety of the patient or others if those family members are in a position to lesson or avert the threat.
- *Moses v. Providence Hospital and Medical Centers, Inc.*: Sixth Circuit decision held that the EMTALA obligation to stabilize and emergency medical condition survives inpatient admission. Also expands right to sue to include anyone who is injured as a "direct result" of the violation.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

February 2016 Regulations

- Proposed rule would revise 42 CFR, Part 2 (Confidentiality of Alcohol and Drug Abuse Patient Records).
- Authorizing statute (42 U.S.C. Section 290dd-2) protects the confidentiality of the identity, diagnosis, prognosis or treatment of any patient records which are maintained in connection with the performance of any federally assisted program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation or research.
- Last update was 1987.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

February 2016 Regulations continued

- The laws and regulations governing confidentiality of substance abuse records were written out of great concern about the potential use of this information against individuals, causing them to avoid needed treatment.
- Negative consequences of disclosure includes loss of employment, loss of housing, loss of child custody, discrimination by medical professionals and insurers, arrest and incarceration.
- Proposed rule would make policy changes to the regulations to better align them with advances in the U.S. health care delivery system while retaining important protections.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

February 2016 Regulations continued

- Purpose is to modernize rules by facilitating the electronic exchange of substance use disorder information for treatment and other legitimate health care purposes while ensuring appropriate confidentiality protections for records that might identify an individual, directly or indirectly, as having or having had a substance use disorder.
- SAMHSA proposed to define the term "substance use disorder" in such a manner as to cover substance use disorders that can be associated with altered mental status that has the potential to lead to risky and/or socially prohibited behaviors.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

February 2016 Regulations continued

- "Treating provider relationship" means that, regardless of whether there has been an actual in-person encounter.
- A patient agrees to be diagnosed, evaluated and/or treated for any condition by an individual or entity, and
- The individual or entity agrees to undertake diagnosis, evaluation and/or treatment of the patient, or consultation with the patient, for any condition.
- An agreement might be evidenced, among other things, by making an appointment or by a telephone consultation.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

February 2016 Regulations continued

- Delete the definition of "detoxification treatment" and replace it with the definition of the currently acceptable term "withdrawal management."
- Expand the definition of "patient."
- Delete the speed with which information could identify a patient and focus only on the information.
- Revise the definition of "Records" to include any information whether recorded or not, received or acquired by, an applicable program relating to a patient. This includes both paper and electronic records.

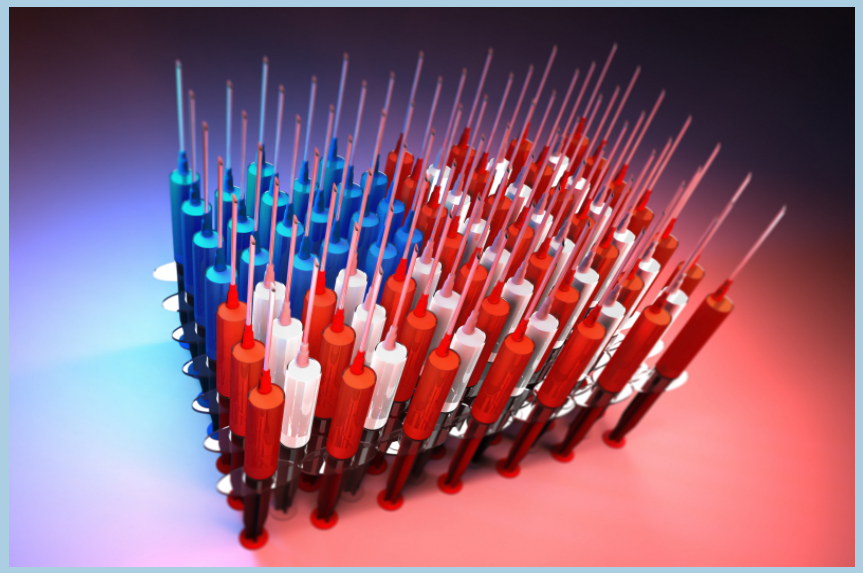
Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

February 2016 Regulations *delayed*

- February 16, 2017 Federal Register: Delays the effective date of these regulations until March 21, 2017.
- In accordance with the "Regulatory Freeze Pending Review." (82 Federal Register 6052 (Jan. 18, 2017).

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT



And yet to every bad there's a worse.

-- Thomas Hardy

The HITECH Act– Introduction

- The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.
- HITECH addressed the privacy and security concerns associated with the electronic transmission of health information through several provisions designed to strengthen the civil and criminal enforcement of HIPAA.
- Modified the authority of HHS to impose civil money penalties for violations occurring after February 18, 2009.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Enforcing HIPAA

Press Release – October 30, 2009

- "The Department's implementation of these HITECH Act enforcement provisions will strengthen the HIPAA protections and rights related to an individual's health information," said Georgina Verdugo, the director of OCR.
- This strengthened penalty scheme will encourage health care providers, health plans and other health care entities required to comply with HIPAA to ensure that their compliance programs are effectively designed to prevent, detect and quickly correct violations of the HIPAA rules," said Verdugo. "Such heightened vigilance will give consumers greater confidence in the privacy and security of their health information and in the industry's use of health information technology."

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH Revises HIPAA

- HITECH established four categories of violations that reflect increasing levels of culpability.
- Created four corresponding tiers of penalty amounts that significantly increased the minimum penalty for each violation.
- A maximum penalty amount of $1.5 million for all violations of an identical provision.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH Revises HIPAA continued

- Eliminated the previous bar on the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation.
- Provided a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH Revises HITECH in 2013

- The HITECH Act defines a "breach" as the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information.
- The interim final rule required covered entities and business associates to perform a risk assessment and required notification only if the incident resulted in a significant risk of financial, reputational or other harm to the individual.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH revises HITECH in 2013 continued

- The final rule replaces the harm standard of the interim final rule with a presumption that any use or disclosure of PHI not permitted by HIPAA is a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised.
- This determination must be based on a risk assessment that considers at least the following factors:

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH revises HITECH in 2013 continued

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH revises HITECH in 2013 continued

- The final rule imposes on business associates the obligation to enter into and follow business associate agreements with each covered entity. Business associates may use and disclose PHI only as permitted or required by their business associate contracts or as required by law.
- Business associate agreements should describe all the contemplated uses and disclosures of PHI by the business associate.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH revises HITECH in 2013 continued

- The final rule expands the reach of HIPAA's business associate requirements by broadening the definition of a business associate to include persons receiving protected health information from a business associate to perform legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.
- The final rule does not require covered entities to enter into business associate agreements with their business associate's subcontractors, but the business associate will need such an agreement with each subcontractor.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HITECH revises HITECH in 2013 continued

- The final rule requires covered entities to modify their notice of privacy practices s to advise affected individuals of several privacy protections, including:
- New authorization requirements for sales of PHI, marketing and psychotherapy notes;
- The right of an individual to restrict disclosures of PHI to a health plan for health care for which the individual has paid out of pocket;
- The duty of a covered entity to provide notice of a breach of unsecured PHI; and
- The right to opt out of fundraising communications.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

OFFICE OF CIVIL RIGHTS

Justice without force is powerless; force without justice is tyrannical.

-- *Blaise Pascal*

The OCR Today

- Before 2016, the OCR was only investigating non-compliance situations after a complaint, tip, or media report had been filed.
- As a result, 98% of closed privacy cases were the result of a complaint. The HITECH audit act was effective starting in 2010, but the OCR had yet to implement an audit program that would proactively evaluate the compliance status of covered entities and business associates.
- A 2015 report released by the Office of Inspector General found the OCR's oversight of HIPAA compliance to be lacking.
- Now, the OCR plans to strengthen its review efforts by implementing a second phase of audits that was scheduled to occur in 2014, but encountered a number of delays.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

The OCR Today continued

- In this new round of assessments, providers with fewer than 15 physicians and health care business associates will be subject to audits.
- A business associate is any person or group that generates, stores, receives, or transmits PHI on behalf of the covered entity with which they're affiliated. A covered entity is any health plan, healthcare clearinghouse, or healthcare provider that electronically transmits PHI.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Guidance from the OCR

Guidance Regarding Methods for De-identification of PHI in Accordance with the HIPAA Privacy Rule

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

Research

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/research/research.pdf

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Guidance from the OCR continued

Public Health

- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/publichealth/publichealth.pdf

Health Information Technology

- https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Guidance from the OCR continued

Genetic Information Nondiscrimination Act (GINA)

- https://www.gpo.gov/fdsys/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf

2013 Modifications to HIPAA Privacy, Security, Enforcement and Breach Notification Rules under HITECH and GINA

- https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Guidance from the OCR continued

HIV and HIPAA

- https://www.aids.gov/privacy/

National Instant Criminal Background Check System (NICS)

- https://www.hhs.gov/hipaa/for-professionals/special-topics/NICS/index.html
- On January 4, 2016, HHS modified the Privacy Rule to expressly permit certain covered entities to disclose to the NICS the identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a firearm.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Guidance from the OCR continued

LGBT Plus

- https://www.hhs.gov/sites/default/files/hipaa-and-marriage.pdf

Mobile Health Apps Developers

- https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

Cloud Computing

- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

CLIA

Clinical Laboratory Improvement Amendments of 1988 (CLIA)

- 2014 regulations amended CLIA to allow laboratories to give a patient, or a person designated by the patient, his or her "personal representative," access to the patient's completed test reports on the patient's or patient's personal representative's request.
- At the same time, these regulations eliminated the exception under the Privacy Rule to an individual's right to access his or her PHI when it is held by a CLIA-certified or CLIA-exempt laboratory.
- Changes gave patients a new option to obtain their test reports directly from the laboratory while maintaining strong protections for patients' privacy.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

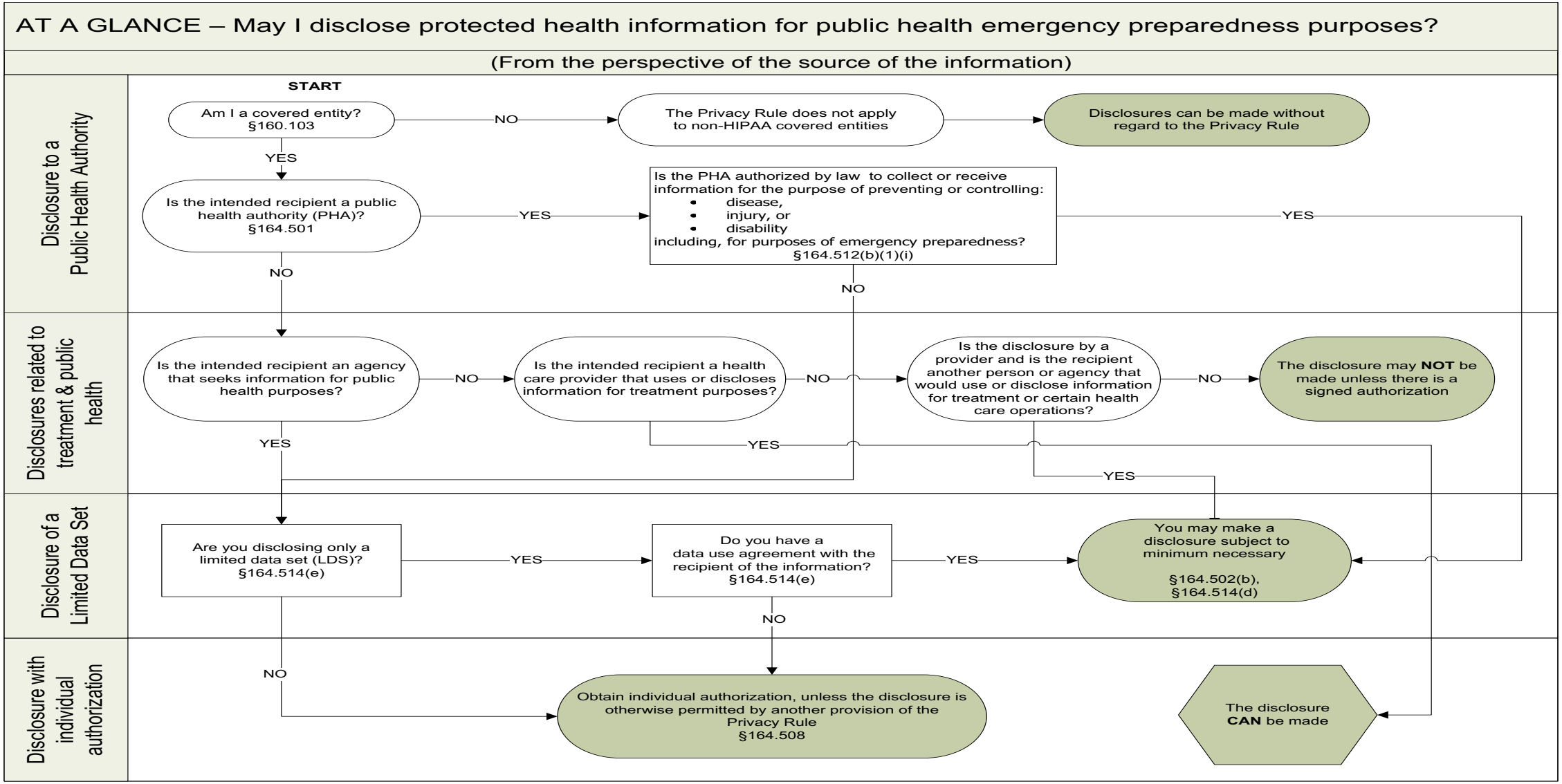
Emergency Planning and Response

- Planning for emergency situations includes gaining access to and using health information about persons with disabilities or others consistent with the Privacy Rule.
- HIPAA privacy in emergency situations

  https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/hipaa-privacy-emergency-situations.pdf
- A Guide for Law Enforcement

  https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/katrinanhipaa.pdf

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP



Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Nondiscrimination Laws and Emergencies

Persons with special needs or who are at risk in an emergency include:

- Children
- Elderly persons
- Persons from diverse cultural origins
- Individuals with disabilities
- Individuals with limited English proficiency
- Persons who live in institutionalized settings
- Persons who do not have access to transportation

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Waivers

If the President declares an emergency or disaster *and* the Secretary of HHS declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the Privacy Rule. The Privacy Rule remains in effect. The waivers are limited and apply only for limited periods of time.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Waivers – What?

- The requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care (45 CFR § 164.510(b))
- The requirement to honor a request to opt out of the facility directory (45 CFR § 164.510(a))
- The requirement to distribute a notice of privacy practices (45 CFR § 164.520)
- The patient's right to request privacy restrictions (45 CFR § 164.522(a))
- The patient's right to request confidential communications (45 CFR § 164.522(b))

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Waivers – When and to What?

- In the emergency area and for the emergency period identified in the public health emergency declaration.
- To hospitals that have instituted a disaster protocol. The waiver would apply to all patients at such hospitals.
- For up to 72 hours from the time the hospital implements its disaster protocol.
- When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours has not elapsed since implementation of its disaster protocol.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HOW FAR HAVE WE COME?

The individual has always had to struggle to keep from being overwhelmed by the tribe.

-- *Friedrich Nietzsche*

What Has the OCR Done?

- Since the compliance date of the Privacy Rule in April 2003, OCR has received over 150,507 HIPAA complaints, resolving 98% of these cases (147,826).

- OCR has investigated and resolved over 24,879 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

What Has the OCR Done? continued

- To date, OCR has settled cases resulting in a total dollar amount of $67,210,982.00.

- OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA in the News (2017)

- Overlooking risks leads to breach -- $400,000 settlement (April 12, 2017)
- $5.5 million HIPAA settlement shines light on the importance of audit controls (February 16, 2017)
- Lack of timely action risks security and costs money (February 1, 2017)
- First HIPAA enforcement action for lack of timely breach notification settles for $475,000 (January 9, 2017)

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA in the News (2016)

- UMass settles potential HIPAA violations following malware infection (November 22, 2016)
- $2.14 million HIPAA settlement underscores importance of managing security risk (October 17, 2016)
- HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements (September 23, 2016)
- Advocate Health Care settles potential HIPAA penalties for $5.55 million (August 4, 2016)

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA in the News (2016) continued

- Multiple alleged HIPAA violations result in $2.75 million settlement with the U. of Miss Medical Center (July 21, 2016)
- Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University (July 18, 2016)
- Unauthorized filing for "NY Med" results in $2.2 million settlement with New York Presbyterian Hospital (April 21, 2016)
- $1.55 million settlement underscores the importance of executing HIPAA business associate agreements (March 17, 2016)

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

HIPAA in the News (2015)

- $750,000 HIPAA settlement underscores the need for organization wide risk analysis (December 14, 2015)
- Triple-S Management Corporation settles HHS charges by agreeing to $3.5 million HIPAA settlement (November 30, 2015)
- HIPAA settlement highlights importance of safeguards when using internet applications (July 10, 2015)
- HIPAA settlement highlights the continued importance of secure disposal of paper medical records (April 30, 2015)

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Sutter Health

- When a thief stole an unencrypted desktop computer from Sutter Health containing the patient information of over 4 million patients, one of the largest class actions to date followed.
- In 2014 the California Court of Appeal dismissed the 13 class action lawsuits seeking over $4 billion in damages because Sutter Health did not intend to disclose the compromised information, and the court ruled that loss of the unencrypted computer alone was "not a breach of confidentiality."
- The California Supreme Court rejected review, even though California may never know what came of the 4 million missing patient records.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Presbyterian Hospital and Columbia University

- Someone stumbled across the patient health information of a deceased partner, launching an investigation that ended in a $4.8 million fine against New York and Presbyterian Hospital and Columbia University.
- The fact that the transgression was caused by an errant physician deactivating a personal computer server on a system network did little to mitigate the record-breaking penalty levied against these two institutions.
- In terms of HIPAA, a breach is a breach.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Affinity Health Plan, Inc.

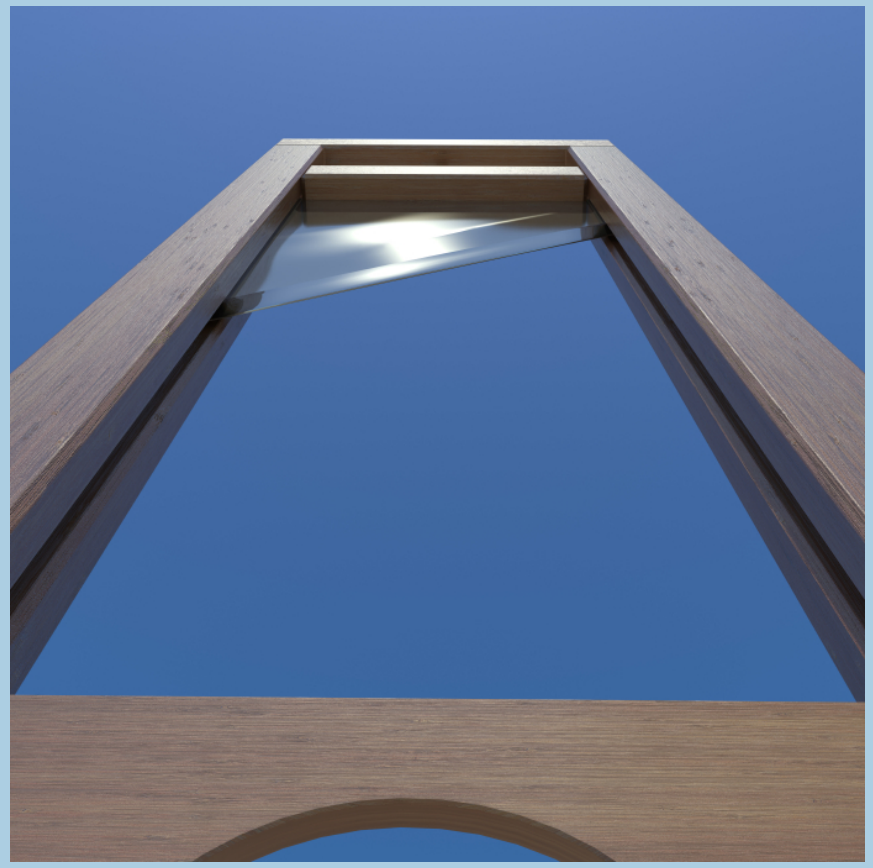
- CBS purchased a photocopier from Affinity Health Plan, Inc. Before releasing the machine, Affinity forgot to delete the stored patient health information of up to 344,579 individuals.
- The resultant fine was $1,215,780.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

CRIMINAL HIPAA

Nothing is easier than denouncing the evildoer. Nothing more difficult than understanding him.

-- *Fyodor Dostoyevsky*



Patient Health Information Gone Rogue

- Over 600 criminal referrals from OCR to DOJ.
- Small percentage prosecuted in the past, but this number is on the rise.
- Typically requires *knowing disclosure* + *personal gain*.
- 42 U.S.C. Section 1320d-6.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

United States v. Benton

- Over a period of 19 months between June 2011 and December 2012, Benton accessed the records of more than 600 patients of Tampa General Hospital without authorization.
- Benton and others copied the personal information of patients and filed fraudulent tax returns in the names of 29 patients.
- In total, false tax returns of $226,000 were sought. In addition to a 37-month prison sentence, Benton was required to pay back $77,239.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Not As Rogue: *United States v. Zhou*

- Unauthorized access alone triggered criminal charges.
- UCLA cardiologist terminated, then reviewed medical records for his co-workers and A-List Hollywood stars – 323 times in three weeks.
- Violation was a misdemeanor – no personal profit or fraud – received 4-month prison sentence.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Other Prosecutions

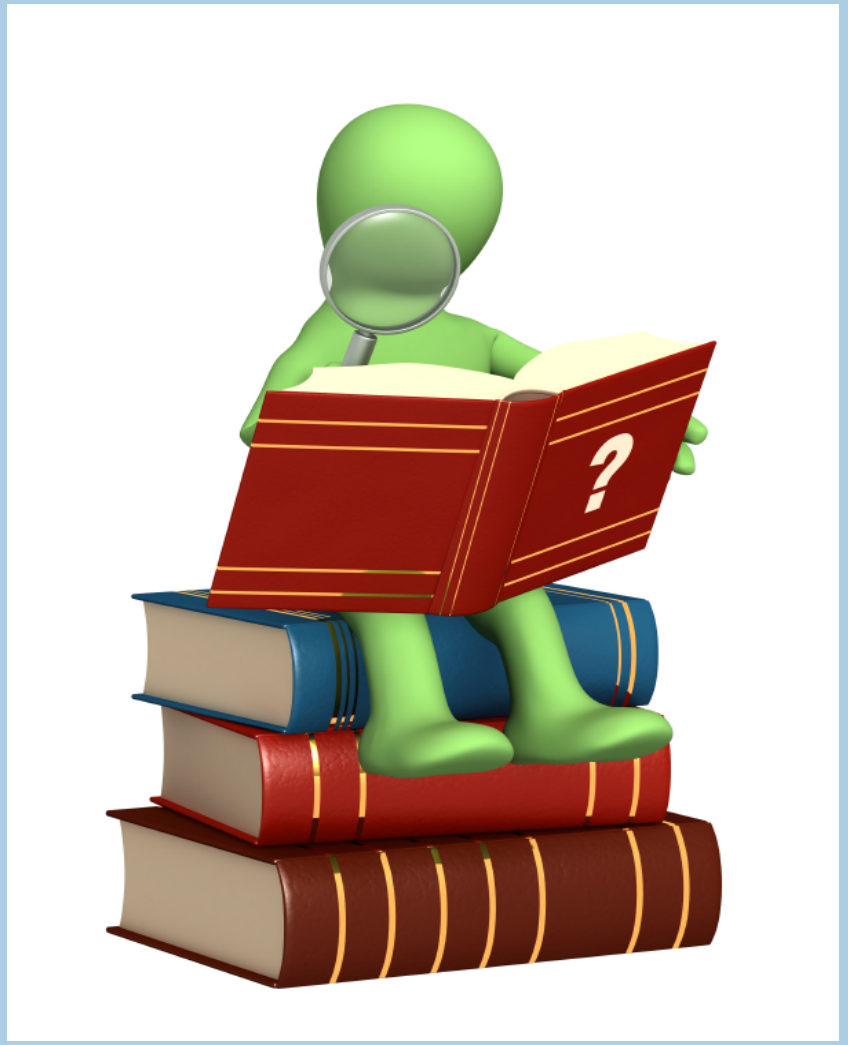
- In April 2013, Helene Michel, the former owner of a Long Island, NY medical supply company, was sentenced to 12 years in prison that involved $10.7 million in Medicare fraud as well as criminal HIPAA violations.
- In November 2014, Christopher Lykes, Jr., a former South Carolina state employee, was sentenced to three years of probation, plus community service, after he sent personal information about more than 228,000 Medicaid recipients to his personal e-mail account.
- In February 2015, Joshua Hippler of Longview, Texas was sentenced to 18 months in federal prison for criminal HIPAA violations. FromDecember 2012 through January 2013, Hippler obtained PHI and attempted to use it for his personal gain.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

PRIVACY LAWS AROUND THE WORLD

If you have ten thousand regulations you destroy all respect for the law.

-- *Winston Churchill*



Europe and Eurasia (non–EEA)

- With the recent adoption of the European General Data Protection Directive (GDPR), attention of the business community has been focused on changes to the privacy rules in the 28 members states of the European Union (and as well as Switzerland and the other members of the European Economic Area or EEA).
- However, these changes are likely to have a ripple effect on existing privacy laws in the 17 jurisdictions in Europe and Eurasia that are not part of the EU or EEA: Albania, Andorra, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Georgia, Kosovo, Macedonia, Moldova, Monaco, Montenegro, Russia, San Marino, Serbia, Turkey and Ukraine.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Europe and Eurasia: Common Elements

- All of the laws in the region include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.
- Legal bases include: (1) consent; (2) legitimate interests; (3) vital interests or necessary to comply with a legal requirement.
- Organizations that collect, use and disclose personal information must take reasonable precautions to protect that information from loss, misuse, authorized access, disclosure, alteration or destruction.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Right to Be Forgotten

- Russia passed its right to be forgotten law in July 2015. The law requires that a search engine remove links to information that is unreliable or false, outdated or irrelevant, or posted in violation of the law.
- Search engines have ten days to either remove the links or provide a reasoned explanation for refusal. Search engines that violate the law are subject to fines from 80,000 to 100,000 rubles ($1,210-$1,512) if they refuse to remove the links at the individual's request and fines of 800,000 to 1 million rubles ($12,098-$15,123) if they violate a court order to remove the links.
- Since the law passed, 73 percent of requests have been denied by Yandex LLC – Russia's leading search engine.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

East, Central and South Asia and the Pacific

- Thirteen jurisdictions in Asia now have comprehensive privacy laws: Australia, Hong Kong, India, Japan, Kazakhstan, Kyrgyzstan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea and Taiwan. New Zealand is the only jurisdiction in the region that has been recognized by the European Commission as providing adequate protection.
- Notably absent from this list are countries such as China, Thailand, Vietnam and Indonesia.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Latin America, Caribbean and Canada

- Fifteen jurisdictions now have comprehensive privacy laws including: Antigua and Barbuda, Argentina, Aruba, Bahamas, Canada, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Mexico, Nicaragua, Peru, Trinidad and Tobago (currently, the only provisions in force pertain to the establishment of the data protection authority) and Uruguay.
- Saint Lucia adopted legislation in 2011, but the law hasn't yet gone into effect.
- The laws in Argentina, Canada and Uruguay have been deemed by the European Commission to provide adequate protection.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Africa and the Near East

- Eighteen countries have enacted comprehensive privacy laws: Angola, Benin, Burkina Faso, Cape Verde, Cote D'Ivoire, Gabon, Ghana, Israel, Madagascar, Mali, Mauritius, Morocco, Qatar/Qatar Financial Centre, Senegal, Seychelles, South Africa, Tunisia and the United Arab Emirates/Dubai International Financial Centre.
- All but the South African law, which has not yet entered into force, are in effect.
- With the adoption in June 2014 of the African Union (AU) Convention on cybersecurity and data protection, more countries in the region are likely to enact their own comprehensive privacy laws regulating the collection and use of personal information by the private sector.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

KILLING HIPAA

The evolution of sense is, in a sense, the evolution of nonsense. -- *Vladimir Nabokov*

Is HIPAA Necessary?

- Before HIPAA takes its next evolutionary step, modern medicine must ask itself if it is worse to fail in the attempt to protect that which is held sacred by law or ignore the transgressions occurring below the surface that so desperately need to be targeted.
- To heal the body it may also be necessary to treat the mind, but HIPAA only protects both when medicine recognizes one as a comorbidity of the other. When this is not the case, all of HIPAA's power slices the treatment in half, at least in terms of confidentiality.
- What remains of the act's reach may be ineffective in light of it's ultimate intent.

Craig B. Garner, Garner Health Law Corporation
Grant B. Gelberg, Huang Ybarra Singer & May LLP

Craig B. Garner Garner Health Law Corporation

- Craig is an attorney and health care consultant, specializing in issues pertaining to modern American health care and the ways it should be managed in its current climate of reform.
- Craig's law practice focuses on health care mergers and acquisitions, regulatory compliance and counseling for providers. Craig is also an adjunct professor of law at Pepperdine University School of Law, where he teaches courses on Hospital Law and the Affordable Care Act.
- Between 2002 and 2011, Craig was the Chief Executive Officer of Coast Plaza Hospital in Norwalk, California. Craig is also a Fellow with the American College of Healthcare Executives.
- Additional information can be found at www.garnerhealth.com.

Grant B. Gelberg Huang Ybarra Singer & May LLP

- Grant B. Gelberg is a partner of Huang Ybarra Singer & May LLP. Mr. Gelberg has significant jury trial experience and focuses his practice on white collar criminal defense, health care enforcement matters, internal corporate investigations, and complex civil litigation.
- Prior to joining Huang Ybarra Singer & May LLP, Mr. Gelberg served as an Assistant United States Attorney in the Major Frauds section of the U.S. Attorney's Office in Los Angeles. In that role, he investigated and prosecuted white collar crimes, including health care fraud, bank fraud, tax fraud, insurance fraud, and large-scale identity theft. Mr. Gelberg also served as a Special Agent with the U.S. Department of Health & Human Services, Office of Inspector General and received specialized training in conducting federal criminal investigations.
- Mr. Gelberg is a member of the Health Care Law Committee of the California State Bar's Business Law Section, the Federal Bar Association, and the American Bar Association's White Collar Crime Committee. He is admitted to practice in California, the U.S. District Court for the Central District of California, and the Ninth Circuit Court of Appeals.

THANK YOU

Garner Health Law
CORPORATION

1299 Ocean Avenue, Suite 450
Santa Monica, CA 90401
310-458-1560
craig@garnerhealth.com
www.garnerhealth.com

HYSM
HUANG YBARRA SINGER & MAY LLP

550 South Hope Street, Suite 1850
Los Angeles, CA 90071
213-884-4900
grant.gelberg@hysmlaw.com
www.hysmlaw.com