GT GreenbergTraurig

Cybersecurity in the Health Care Sector

Corporate Compliance Symposium

Home Care Association of New York State &
Hospice and Palliative Care Association of New York State

October 17, 2018

Francis J. Serbaroli | serbarolif@gtlaw.com | 212.801.2212

Cyberattacks on Rise in Health Care

- HHS: As of 2015, more than 112 million medical records compromised
- Identity Theft Resources Center
  - 1293 data breaches in United States in 2017, 20% more than 2016

Business	50.5%
Medical/Healthcare	28.3%
Education	8.8%
Banking/Credit/Financial	7.1%
Government/Military	5.3%

CRYPTONITE: Major IT/Hacking Events attributed to ransomware by health care institutions increased 89% from 2016 to 2017

© 2018 Greenberg Traurig, LLP

Cyberattacks have struck

- Hospitals & Health Systems
- Health Insurers, Managed Care Plans, Union Benefit Plans
- Clinical Laboratories
- Pharmacies & Pharmacy Benefit Managers
- Nursing Homes
- Home Health Agencies
- Physician Practice Groups
- Renal Dialysis Providers
- Medical Billing Companies & Third Party Administrators

© 2018 Greenberg Traurig, LLP

Healthcare Approaching 20% of GDP

- Repository for enormous amounts of valuable data and information
- Example: Health Care Systems
  - Patient information
    - personal
    - medical
    - financial
  - Confidential internal information:
    - quality assurance
    - risk management
    - incident reports
    - confidential business and financial information
    - confidential board and medical staff committee minutes
    - physician and clinician credentials files
    - employee personal and financial information
    - strategic planning information
    - pricing information

© 2018 Greenberg Traurig, LLP

Patient Safety

- Cyberattackers can:
  - can be external or even internal
  - can access internal data such as physician names and license numbers, Drug Enforcement Agency (DEA) numbers, pharmacy licenses, and generate fraudulent e-mails directing payment of money, transfers of drugs, and other transactions.
  - can shut down access to electronic patient records
  - can disrupt software & proper functioning of medical equipment connected to internet (e.g. monitors, pacemakers)
  - can intercept & disrupt telemedicine consultations

© 2018 Greenberg Traurig, LLP

Lucrative Market

- Some experts believe PHI is more valuable than Social Security numbers or personal financial information
  - Experian: Social Security Number - $1 each

    Medical Record - $1-$1,000
- Criminals use PHI for frauds & scams:
  - create fraudulent health insurance claims
  - fraudulent purchases & resales of medical devices or equipment
  - gain access to prescription drugs for their own use or resale on black market

© 2018 Greenberg Traurig, LLP

Federal Health Care Industry Cybersecurity Task Force Report

June 2017

Many health care organizations:

> "lack the infrastructure to identify and track threats, the capacity to analyze and translate the threat data they receive into actionable information, and the capability to act on that information. Many organizations also have not crossed the digital divide in not having the technology, resources and expertise to address current and emerging cybersecurity threats. These organizations may not know that they have experienced an attack until long after it has occurred."

© 2018 Greenberg Traurig, LLP

Ransomware

- A type of malware that infects IT systems and files, and makes them inaccessible until a ransom is paid. The target can't access critical patient data and has to use paper records for the duration.
- Ransomware attacks can be:
  - a malicious attachment to a phishing e-mail
  - a malicious link accessed by someone at the target
  - an advertisement containing malware

© 2018 Greenberg Traurig, LLP

Distributed Denial of Service (DDoS) Attacks

Cyberattackers overwhelm a target's IT network to make it inoperable. It can prevent access to the Internet, prevent the sending or receipt of e-mails, and disrupt the transmission of medical records, information, prescriptions and orders, etc.

© 2018 Greenberg Traurig, LLP

HIPPA Privacy Rule– 45 CFR §164.501 et seq.

- Protects all individually identifiable health information held or transmitted by covered entity or its business associate in any form or media, whether electronic, paper or oral.
- Personal health information (PHI) includes information about:
  - the patient's past, present or future physical health or condition
  - the health care provided to the patient
  - the past, present or future payment for the health care services provided
  - includes name, address, Social Security Number

© 2018 Greenberg Traurig, LLP

HIPPA Security Rule– 45 CFR Parts 160 and 164(A) and (C)

The Security Rule applies to:

- any health care provider
- health plan
- health care clearing houses
- It mandates that covered entities and business associates and their respective work forces ensure the confidentiality of all electronic health records using appropriate physical and electronic safeguards.
- This includes identifying and protecting against any reasonably anticipated threats or hazards to the security or integrity of such records; and protecting against reasonably anticipated impermissible uses or disclosures.
- The Security Rule applies to all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits.

© 2018 Greenberg Traurig, LLP

HIPPA Breach Notification Rule – 45 CFR §§164.400-414

Definition of Breach

"A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment . . ."

© 2018 Greenberg Traurig, LLP

HIPPA Breach Notification Rule – 45 CFR §§164.400-414 (cont'd)

Requirements

- Notify HHS if the breach involved unsecured protected health information, i.e. information that has not been rendered unusable, unreadable, or indecipherable to unauthorized person.

© 2018 Greenberg Traurig, LLP

HIPPA Breach Notification Rule – 45 CFR §§164.400-414 (cont'd)

Requirements

- Notify affected individuals in writing via first class mail (or by e-mail if affected individuals have agreed to receive such notices electronically) without unreasonable delay and in no case later than 60 days following discovery of the breach.
- Notice to individuals must include, to the extent possible:
  - A brief description of the breach;
  - The types of information involved;
  - The steps they should take to protect themselves;
  - What the entity is doing to investigate the breach, mitigate harm, and prevent further breaches; and
  - How individuals can contact the entity that was breached..

© 2018 Greenberg Traurig, LLP

HIPPA Breach Notification Rule – 45 CFR §§164.400-414 (cont'd)

Requirements

- The entity must notify prominent media outlets serving the locale if the breach involves more than 500 residents. Media notification must be made without unreasonable delay and in no case later than 60 days following the discovery of the breach, and include the same information required in the individual notification.
- Notify HHS via electronic form on HHS website:
  - If breach affects 500 or more, the entity must notify HHS without unreasonable delay but in case later than 60 days following the breach.
  - If breach effects fewer than 500, notify HHS on an annual basis no later than 60 days after end of calendar year.

IMPORTANT! Maintain documentation that all required notifications to individuals were made.

© 2018 Greenberg Traurig, LLP

HIPPA Breach Notification Rule – 45 CFR §§164.400-414 (cont'd)

Enforcement & Penalties

- HHS' Office of Civil Rights enforces HIPAA.
- Violations can trigger significant Civil Monetary Penalties: $100 to $50,000 or more for each violation depending upon facts.
- Department of Justice can prosecute criminal violations.

© 2018 Greenberg Traurig, LLP

FEDERAL TRADE COMMISSION (FTC) HEALTH BREACH NOTIFICATION RULE – 16 CFR Part 318

- In health care, the FTC Notification Rule applies only to:
  - a vendor of personal health records (PHR);
  - a PHR-related entity; or
  - a third party service provider for a vendor of PHRs or PHR-related entity
- FTC Notification Rule does not apply to any person or entity covered by HIPAA.
- FTC must be notified of any unauthorized acquisition of PHR-identifiable health information that is unsecured and in a PHR.

© 2018 Greenberg Traurig, LLP

FEDERAL TRADE COMMISSION (FTC) HEALTH BREACH NOTIFICATION RULE – 16 CFR Part 318 (cont'd)

Requirements

- Breach involving 500 or more individuals:
  - Notify each affected citizen or resident of USA without unreasonable delay but within 60 days after discovery of breach.
  - Notify FTC via electronic form on FTC website as soon as possible but within 10 business days after discovery of breach.
  - Notify prominent media outlets serving the locale, including internet media, without unreasonable delay but within 60 calendar days of discovery of breach.
- Breach involving fewer than 500 individuals:
  - Notify FTC within 60 calendar days after end of calendar year.

© 2018 Greenberg Traurig, LLP

Securities and Exchange Commission (SEC) Notification

- If the covered entity or business associate has publicly-traded stock and the breach is material, it must be disclosed in SEC filings (10-K and 10-Q)
- (SEC itself was hacked in 2016 but did not publicly disclose the hack until September 20, 2017.)

© 2018 Greenberg Traurig, LLP

New York's Medical Information Confidentiality Protections

- Public Health Law §18
  - Sets forth the circumstances under which medical records may be released to third parties with (or sometimes without) the consent of the patient (or person authorized by patient).

© 2018 Greenberg Traurig, LLP

10 NYCRR § 763.2 (a) Rights of Home Care Patients

- Rights of home care patients include:
  - (10) privacy, including confidential treatment of patient records, and refusal of their release to any individual outside the agency except in the case of the patient's transfer to a health care facility, or as required by law or third party payment contract;

© 2018 Greenberg Traurig, LLP

New York's Medical Information Confidentiality Protections (cont'd)

- It is advisable to promptly notify DOH of any significant breach of patient information or of any external shutdown of access to electronic medical records, as these events affect the agency's ability to provide code-compliant health care services.
- It is better for the DOH to learn about a breach directly from the agency rather than from HHS or media reports.

© 2018 Greenberg Traurig, LLP

New York's Medical Information Confidentiality Protections (cont'd)

- Mental Hygiene Law §33.13
  - Strictly limits disclosures of records of mental health treatment.
- Public Health Law §2782-2784
  - Strictly limits disclosures of HIV-related information.
- Public Health Law §4410(3)
  - Special rules applying to reports about child abuse and mistreatment.

© 2018 Greenberg Traurig, LLP

New York's Medical Information Confidentiality Protections (cont'd)

- 11 NYCRR §420.17 and 420.10
  - Insurers restricted from disclosing non-public personal health and financial information.
- Civil Practice Law & Rules (CPLR) §4504 (Litigation)
  - No physician, nurse, dentist, podiatrist or chiropractor may disclose any information acquired in attending a patient in a professional capacity unless the patient waives the practitioner-patient privilege

© 2018 Greenberg Traurig, LLP

New York's Breach Notification Requirements

- General Business Law §899-aa
  - Defines private information as:
    - Social Security Number
    - Driver's license number or non-driver's identification number
    - Account number, credit or debit card number in combination with security or access code or password

© 2018 Greenberg Traurig, LLP

New York's Breach Notification Requirements (cont'd)

Notification Requirements

- Any person or business that is doing business in New York or has private information in its computerized data must disclose any breach to the affected individuals following discovery or notification of the breach.
- The entity must notify any New York resident whose private information was, or is reasonably believed to have been acquired by an unauthorized person. Disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures needed to determine the scope of the breach and restore the integrity of the system.

© 2018 Greenberg Traurig, LLP

New York's Breach Notification Requirements (cont'd)

Notification Requirements (cont'd)

- Notification must include contact information for the business and a description of the private information that was or may have been compromised.
- Notification may be delayed if a law enforcement agency determines that it would impede a criminal investigation.

© 2018 Greenberg Traurig, LLP

New York's Breach Notification Requirements (cont'd)

Methods of Notification

- Written
- Electronic, but only if the affected individual consents (log must be kept)
- Telephone (log must be kept)

© 2018 Greenberg Traurig, LLP

New York's Breach Notification Requirements (cont'd)

Methods of Notification (cont'd)

- Substitute Notification
  - To be eligible for Substitute Notification, the breached entity must demonstrate to the Attorney General:
    - that the cost of notification would exceed $250,000; or
    - that the number of persons affected exceeds 500,000; or
    - that the business does not have sufficient contact information on the affected individuals.
  - The entity may then make notification:
    - by e-mail if it has the affected individual's e-mail address;
    - by conspicuous posting of notice of the breach on the entity's website; and
    - by notification to major statewide media.

© 2018 Greenberg Traurig, LLP

New York's Breach Notification Requirements (cont'd)

Methods of Notification (cont'd)

- Without delaying notification to affected individuals, the business must notify the Attorney General, the Department of State and the State Police as to the timing, content and distribution of the notifications and approximate number of affected individuals.

© 2018 Greenberg Traurig, LLP

New York's Breach Notification Requirements (cont'd)

Enforcement

- Attorney General authorized to seek damages and injunctive relief for violations of this statute.
- Court may award actual and consequential damages to individuals who were entitled to but did not receive notification.
- Knowing or reckless violations can result in penalties of $5,000 - $10,000 per violation, not to exceed $150,000.

© 2018 Greenberg Traurig, LLP

Take-Aways

- Data breaches are not just an "IT" issue; they are a risk management issue. We must emphasize:
  - The importance of effective written policies and procedures, including an incident response plan; education of everyone entering information or having access to patient information; and active involvement of the entities' senior management.
  - The importance of timely breach reporting if the breach falls within a reporting category under federal or state laws or regulations; and timely notifications to affected patients.
  - The importance of risk assessments, and day-to-day operational controls to safeguard patient information, including assessing data security at outside vendors.

© 2018 Greenberg Traurig, LLP

Take-Aways (cont'd)

- The importance of maintaining attorney-client privilege when a breach is discovered and is being investigated, including having outside counsel retain any outside consultants called in to assist in investigating and fixing the breach.
- The importance of making sure that the organization has insurance coverage for cyberattacks, including business interruption insurance, coverage against lawsuits and class actions, and so on.
- The importance of emphasizing to senior executives and governing board members that cybersecurity is their responsibility, not just their IT Department's.

© 2018 Greenberg Traurig, LLP

QUESTIONS?