GW | GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

NEW YORK | NEW JERSEY | CONNECTICUT

GW | GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

Long Island Health Information Management Association

HIPAA and ROI Updates

April 10, 2019

Presented by:

Carmen E. Jule, Esq.

cjule@garfunkelwild.com

Great Neck, NY	Hackensack, NJ	Stamford, CT	Albany, NY
(516) 393-2200	(201) 883-1030	(203) 316-0483	(518) 242-7582

GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

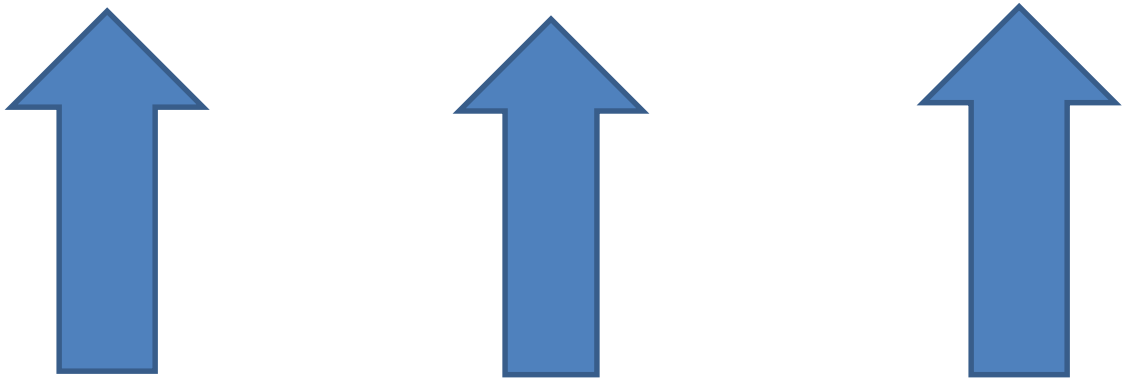
HIPAA Update

OCR Enforcement

- Privacy/Security audits conducted since 2011 by the US-DHHS Office for Civil Rights have largely been educational in nature.
  - Enforcement actions were taken only for deliberate non-compliance.
- OCR officials recently reported that they will be moving away from education and moving toward enforcement.
  - Particular focus will be on physicians who block patient access to medical records.

OCR is Breaking Records

- In 2018, OCR:
  - achieved a record-setting $28.7 million from enforcement actions.
  - Obtained largest single settlement ever ($16 million) from Anthem, Inc.
- Data breaches reported and the number of people whose data is exposed are on the rise.



Data Breaches

- Breaches affecting 500 or more individuals

  86 breaches have been reported in the first three months of 2019 and are currently under investigation by OCR.

Hacking/IT Incident

Unauthorized Disclosure

Unauthorized Access

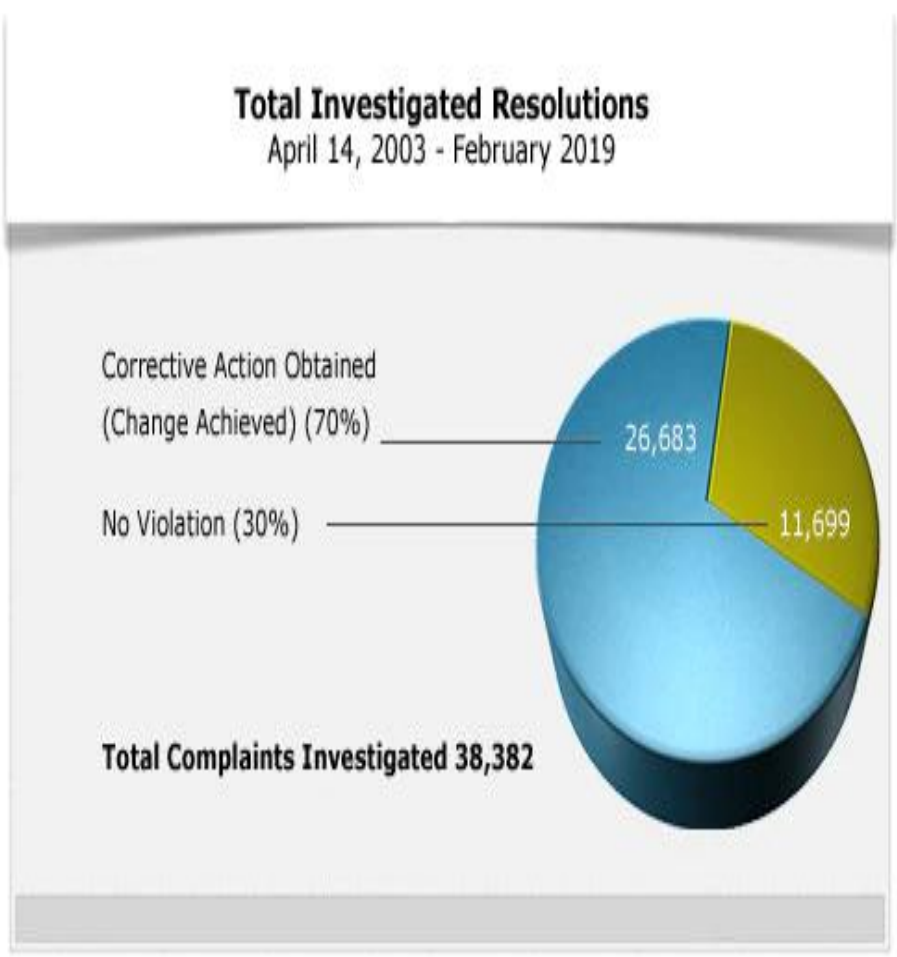
Theft

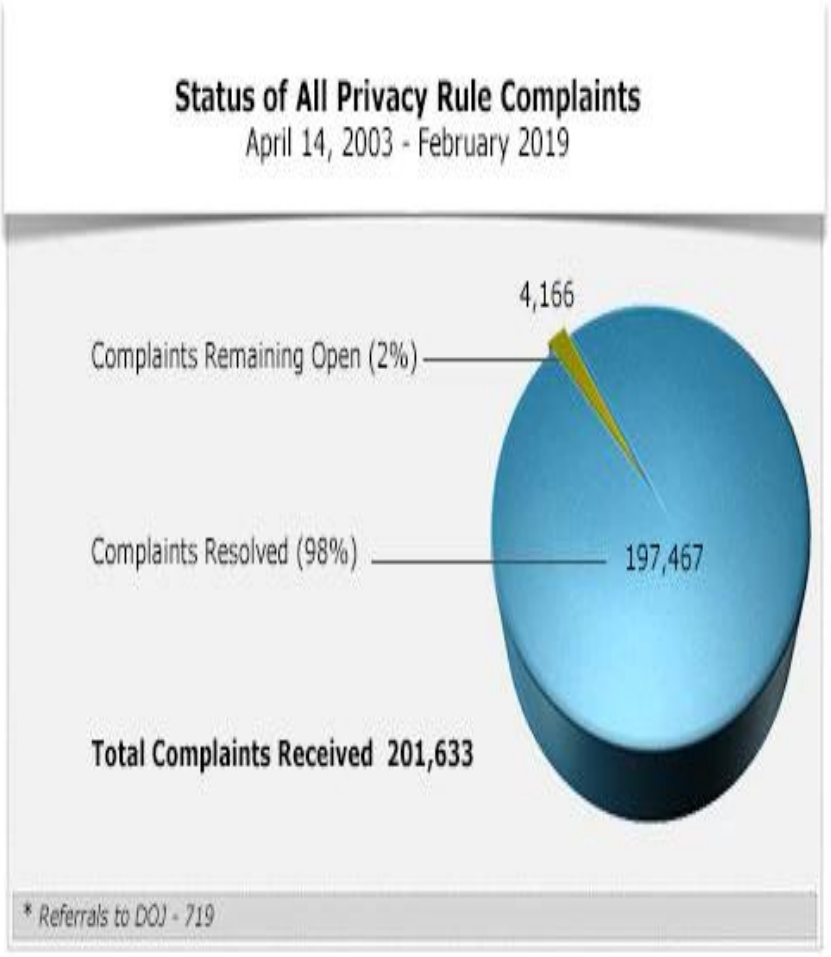
Improper Disposal

Some of the Biggest Health Care Provider Breaches Reported So Far This Year:

Number of Individuals Affected	Type of Breach	Location of Breach
973,024	Hacking/IT Incident	Network Server
400,000	Hacking/IT Incident	Network Server
326,629	Hacking/IT Incident	Email
76,000	Theft	Portable Electronic Device
50,000	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Email, Laptop

OCR Stats





Breach Notification
Examples of Breaches

- A laptop containing unencrypted PHI is left in a car and the car is stolen.
- A receptionist looks up information about her neighbor, at request of the family, even though the receptionist has no work-related reason to do so.
- Staff provides patient with the wrong patient's instructions.
- A Covered Entity's Business Associate fails to implement adequate security mechanisms and the Covered Entity's information is "hacked."
- Disposal of patient information without destroying it properly (e.g., shredding paper, destroying discs) if such patient information is then accessed or used by a third party.

Breach Notification

- Covered Entities are required to inform affected individuals if there is an unauthorized access, use or disclosure of their unsecured PHI.
  - Must be written notification by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
  - Notification must be "without unreasonable delay" and in no case later than 60 days following the discovery of a breach
- Business Associates are required to inform the Covered Entities of such breaches.
- On rare occasions, may be able to avoid notification if the Covered Entity/Business Associate can document a "low probability of compromise" in a risk assessment.

Breach Notification

- If breach affects more than 500 residents of a state or jurisdiction, must provide notice to prominent media outlets.
  - Also "without unreasonable delay" and in no case later than 60 days following the discovery of a breach
- If a breach affects 500 or more individuals, covered entities must notify the HHS Secretary
  - Also "without unreasonable delay" and in no case later than 60 days following the discovery of a breach
- If fewer than 500 individuals affected , the covered entity may notify the HHS Secretary on an annual basis
  - No later than 60 days after the end of the calendar year in which the breaches are discovered.

Recent Breach Settlements

- December 2018: Operator of four California hospitals agreed to pay $3 Million and to adopt a substantial corrective action plan to settle potential violations of the HIPAA Rules.
  - OCR had received notifications regarding two breaches of unsecured electronic protected health information (ePHI) affecting over 62,500 individuals.

Physician Group Settles with OCR

- December 2018: Agrees to pay $500,000 and to adopt a substantial corrective action plan to settle allegations that it did not follow basic security requirements under HIPAA by failing to:
  - enter into a business associate agreement with an individual providing medical billing services;
  - adopt any policy requiring business associate agreements until April 2014; and
  - conduct a risk analysis or implement security measures or any other written HIPAA policies or procedures before 2014 (although it had been in operation since 2005).

Hospital Settles with OCR for $111,400

- December 2018: Also enters into two-year corrective action plan.
- Hospital failed to terminate former employee's access to e-PHI allowing continued remote access to the hospital's web-based scheduling calendar, which contained e-PHI of 557 individuals.
- Also disclosed e-PHI to the web-based scheduling calendar vendor without a HIPAA required business associate agreement in place.

Doctor Discloses PHI to Reporter

- November 2018: Practice agrees to pay $125,000 and to adopt a corrective action plan that includes two years of monitoring of their compliance with the HIPAA Rules.
  - Patient had contacted a local TV station to speak about a dispute that had occurred between the patient and doctor.
  - A reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed patient's PHI to the reporter.

OCR Guidance

- August 2018: OCR Cyber Security Newsletter highlighted the importance of adopting specific policies regarding the effective management of:
  - Mobile devices (*e.g.*, cell phones and laptops)
  - Electronic media (*e.g.*, USB drives and CDs)
    - https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-august-2018-device-and-media-controls.pdf
- To reduce the risk of loss, theft, and the potential of a breach, OCR recommends that organizations consider the following questions when developing policies and procedures:

OCR Guidance

- Is there a record that tracks the location, movement, modifications or repairs, and disposition of devices and media throughout their lifecycles?
- Does the organization's record of device and media movement include the person(s) responsible for such devices and media?
- Are workforce members (including management) trained on the proper use and handling of devices and media to safeguard ePHI?
- Are appropriate technical controls, for example, access controls, audit controls, and encryption, in use?

OCR Guidance

- When determining what security measures to implement, covered entities and business associates must consider the following factors :
  - Its size, complexity, and capabilities.
  - Its technical infrastructure, hardware, and software security capabilities.
  - The costs of security measures.
  - The probability and criticality of potential risks to ePHI.

Cyber Security Guidance

- January 2019: DHHS released "Health Industry Cybersecurity Practices: Managing and Protecting Patients."
  - Four volume publication is a culmination of a two-year collaboration between DHHS and health industry and cybersecurity experts to develop voluntary guidelines aimed at reducing cybersecurity risks and ensuring the security and safety of patients.
  - Provides actionable and practical guidance on cost-effective methods that health care organizations at various size and resource levels can use to reduce cybersecurity risks.

Cyber Security Guidance

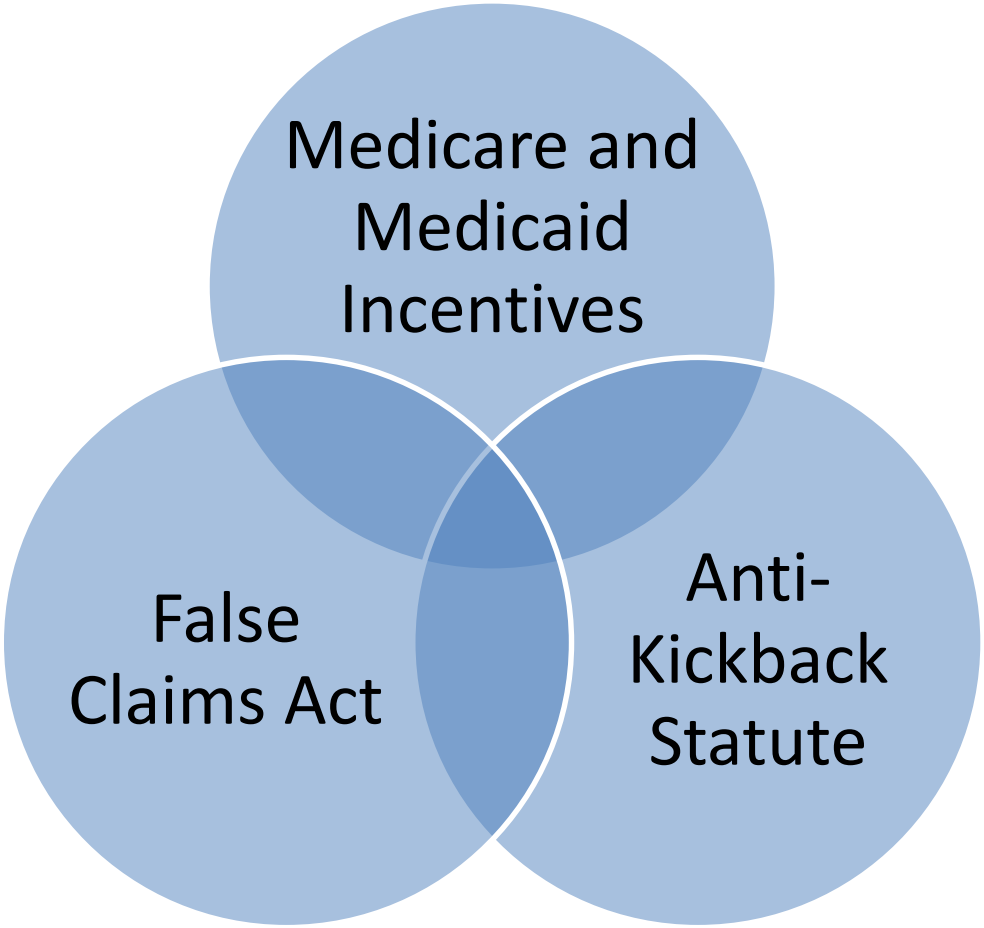
- The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- Technical Volume 1– Cybersecurity Practices for Small Health Care Organizations
- Technical Volume 2 –Cybersecurity Practices for Medium and Large Health Care Organizations
- Resources and Templates

- DHHS's publication is available at:
  - https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

Promoting Interoperability Program (formerly Meaningful Use Program)

- US DHHS Office of Inspector General (OIG) estimates that Medicare has paid more than $729 million in subsidy payments to hospitals and doctors that did not qualify for such payments.
- Audits of Medicaid programs in 14 states found improper payments amounting to $66 million.

What is the Connection Between the Promoting Interoperability Program and Fraud and Abuse?



The Federal False Claims Act (FCA)

- The Federal Government's "Weapon of Choice."
- Provisions prohibit any person from (among other things):
  - knowingly presenting, or causing to be presented, a false or fraudulent claim for payment or approval;
  - knowingly making, using, or causing to be made or used, a false record or statement material to a false or fraudulent claim;
  - knowingly concealing or knowingly and improperly avoiding or decreasing an obligation to pay or transmit money or property to the Government.

The Federal False Claims Act (FCA)

- Permits private parties known as *qui tam* relators to bring an action on behalf of the United States.
- *Qui tam* relators may share in a percentage of the proceeds from the FCA action or settlement.

Major Penalties

- Effective: For assessments made after January 29, 2018, based on associated violations that occurred after November 2, 2015:
  - Minimum penalty: $11,181
  - Maximum penalty: $22,363
  - Per claim.
- Treble damages may also be imposed.

Federal Anti-Kickback Statute

- It is a **crime** to knowingly and willfully –
  - **Solicit or receive, or offer or pay, any remuneration (including any kickback, bribe or rebate) directly or indirectly, overtly or covertly, in cash or in kind, in return for or to induce**:

    - The **referral** of an individual to a person for the furnishing (or arranging for the furnishing) of any item or service for which payment may be made in whole or in part under a **Federal health care program ("FHCP")** (*e.g.*, Medicare or Medicaid);

    - The **purchasing, leasing, ordering or arranging for (or recommending purchasing, leasing or ordering)** any good, facility, service or item for which payment may be made in whole or in part under a **FHCP.**

Federal Anti-Kickback Statute

- What is "remuneration"?
  - The statute specifies:
    - ➢ Kickbacks, bribes, and rebates, whether given directly or indirectly, overtly or covertly, in cash or in kind.
  - But remuneration can be virtually anything of value. Cash and cash equivalents, gift items (*e.g.,* concert/sports tickets, vacations, etc.), above fair-market value payments , free services, etc.
- Certain statutory exceptions and regulatory "safe harbors" protect certain arrangements.

Federal Anti-Kickback Statute: Penalties

- Criminal, civil and administrative penalties may result.
  - The AKS is a **felony crime** and carries a sentence of up to ten years imprisonment, a fine of up to $100,000, or both.
  - The OIG may also impose **administrative penalties** –
    - Currently a maximum of $100,000 for each offer, payment, solicitation, or receipt of remuneration that violates the AKS.
  - Exclusion from Federal health care programs.

Federal Anti-Kickback Statute: Basis for FCA Penalties

- Claims submitted for items or services resulting from a violation of the AKS constitute a "false claim" for purposes of the civil Federal False Claims Act.

FCA/AKS Settlement

- February 2019: Greenway Health LLC, a health information technology and services developer, agreed to pay $57.25 million to resolve claims that it violated:
  - the **Federal False Claims Act** by selling EHR software that didn't meet HHS standards;
    - Allegedly falsified representations to its certifying bodies and users that its software complied with certification requirements and
    - caused its users to falsely attest that they were eligible to receive incentive payments under the meaningful use program.

FCA/AKS Settlement

- Greenway's settlement also resolved allegations that it violated:
  - the Federal **Anti-kickback Statute** by making payments and providing gifts to induce customers to recommend the company and increase its sales.
    - Through its "Ambassador Programs" Greenway allegedly paid favored customers to host site visits, complete reference calls with prospective customers and engage in other promotional activity.
    - Ambassadors were given credits toward their annual fees, either as flat sum amounts or as discounts up to 15% off software support fees.

FCA/AKS Settlement

- Through another program, Greenway allegedly paid referral credits to current users who recommended prospective customers.
- The size of the credit paid was directly tied to the size of the prospective customer; e.g.,
  - Greenway paid $700 for the referral of a one or two physician group and $2000 for the referral of a group of three or more physicians.
- Referral credits were only paid for referrals that actually resulted in a sale.

FCA/AKS Settlement

- According to the government's complaint, Greenway also "lavished gifts" on its most favored customers, e.g.,
  - iPads, meals, travel, tickets to sporting events and entertainment
- The purpose:
  - to induce these customers to either continue using Greenway products or recommend Greenway to other health care providers who would and did use federal health care program funds to purchase Greenway's products and services.

FCA/AKS Settlement

- In entering the settlement agreement with the Department of Justice, Greenway made no admission of liability and denied the government's allegations.

Additional Information for Providers

- The NY State Department of Health advises it is aware of issues with certain Greenway products that have made miscalculations related to NY Medicaid's EHR Incentive Program
  - DOH has stated that deadline accommodations will be provided to impacted Greenway product users for 2018 Meaningful Use attestations.
  - Eligible Professionals should check DOH's website for the Greenway EHR Certification products at issue:
    - https://www.health.ny.gov/health_care/medicaid/redesign/ehr/repository/greenway_list.htm)
  - Providers using any of the listed Greenway product may email hit@health.ny.gov to receive instructions about the attestation process.

Whistleblower Complaint Unsealed

- March 2019: two former employees have blown the whistle on one of the U.S.'s largest publicly traded hospital companies (owns/leases/ operates 127 hospitals in 20 states).
  - The Complaint: The company submitted "hundreds of millions of dollars in false claims" to the US DHHS for federal incentive payments through the Electronic Health Record Incentive Program.
  - The Company: stated the whistleblower allegations are "without merit" and that it has "complete confidence" that all of its meaningful use attestations are "accurate."

Whistleblower Complaint Unsealed: Allegations

- The qui tam plaintiffs allege that the company implemented EHR technology that suffers from "pervasive flaws" that make it ineligible for certification under the Meaningful Use Program.
  - The complaint claims multiple design failures in software for computerized physician order entry and clinical decision support.
    - These flaws prevent healthcare providers from providing clinical care in multiple hospitals safely and reliably.
    - Many create an acute risk to patient health and safety.
      - Software provider (also a defendant) falsely attested to its certifying body that it complied with requirements for Stage 2 certification and payment under the Meaningful Use Program.

Whistleblower Complaint Unsealed: Allegations

- Specifically, the complaint alleges the company received over $450 million in incentive payments between 2012 and 2015 based on false attestations.
  - Defects in software included (to name a few):
    - an inability to calculate weight-based dosing accurately;
    - "send dose now" orders were not scheduled for immediate delivery, but normal delivery at next scheduled frequency;
    - An inability to accurately create PRN medication orders;
    - Unreliable drug-drug, drug-allergy, duplicate therapy and dose range checks.

Whistleblower Complaint Unsealed: Allegations

- An ability for multiple providers to open a patient's chart at the same time (e.g., a physician and pharmacist can make medication orders at the same time which overrides duplication therapy or dose range checking).
- An inability to reliably perform clinical decision support.

- Providers were forced to print clinical information when patients transitioned from one care setting to another as well as when doctors entered medication orders.
- Workflows required nurses to enter the same patient information into the EHR multiple times increasing risk of patient harm.
- The complaint alleges that many more flaws in the EHR software existed and that the company received multiple complaints from its hospital .

Whistleblower Complaint Unsealed

- The Department of Justice is still deciding whether or not it will intervene in the lawsuit.
- Congress' is paying attention: since the complaint was unsealed, the National Coordinator for Health Information Technology has been asked to provide information on processes to ensure compliance with the Promoting Interoperability Program before paying out incentives.
- Others are concerned with how patient care is affected by errors attributed to EHR systems.

Whistleblower Complaint Unsealed

- The civil allegations discussed herein are just that: allegations. The company has denied the allegations against it and has made no admission of liability.

GARFUNKEL WILD, P.C.
ATTORNEYS AT LAW

ROI Litigation Update

Class Action Lawsuit Resolved (for now)

- First filed in 2014.
- Alleged that Healthport Technologies, which contracted with a NY Hospital,* overcharged patient's survivor for copies of medical records in violation of NY Public Health Law Section 18.
- The "circuitous and unusual route" of this litigation over time led a NY Federal District Court to resolve the following questions:

* The hospital was later dropped from the lawsuit.

Class Action Lawsuit Resolved (for now)

- Does Section 18 set a firm 75 cent per-page cap on charges for requests ? **Yes, it does.**
- Does Section 18 categorically authorize a health care provider to charge a requester 75 cents per page regardless of its "costs incurred"? **No, it does not**.
- Does Section 18 require that the provider's charge be no higher than the provider's "costs incurred"? **Yes, it does.**
- May the provider's indirect as well as its direct costs be considered in tabulating its "costs incurred"? **Yes, they may.**

Class Action Lawsuit Resolved (for now)

- On March 14, 2018, a NY Federal District Court resolved the following remaining questions:
  - Does Section 18 prohibit entities other than health care providers from charging above their costs for work responding to patient information requests?
  - **No, it does not. The plain language of the statute imposes duties only on health care providers. A ROI vendor is not barred from profiting from its work assisting a provider to respond to requests for records.**

Class Action Lawsuit Resolved (for now)

- Did Healthport's collaboration with the Hospital – including the contract between them which allowed Healthport to directly bill requesters and retain the 75 cents per-page charge that it billed—give rise to a duty under Section 18 barring Healthport from charging more than its costs incurred?
- **No, the terms of the contract did not mean that Healthport took on any duty under Section 18 to limit its charges to requesters to its own costs incurred.**
  - The contract provided that where state law sets forth per-page fees, Healthport will charge such fees.

Class Action Lawsuit Resolved (for now)

- Did Healthport violate New York's statute prohibiting unfair and deceptive trade practices when it charged survivor $.75 per page for copies of patient's medical records?
- **No, Healthport did not engage in a deceptive or misleading practice by charging more than its costs incurred;**
  - NY's statute governing charges for copies of medical records did not apply to Healthport since it was not a health care provider;
  - contractor's $.75 per page charge matched cap set forth in statute; and
  - Healthport fully disclosed amount of charge to survivor.

Class Action Lawsuit Resolved (for now)

- The plaintiff has filed an appeal with the Federal Court of Appeals (Second Circuit).
- Arguments are scheduled for April 15, 2019.

ROI - Specific Concerns

“I’m the Vice President . . .”

- At a 2017 meeting, Joe Biden relayed the challenge of getting his son Beau’s medical records from one hospital to another.
- “I was stunned when my son for a year was battling stage 4 glioblastoma,” said Biden. “I couldn’t get his records. I’m the vice president of the United States of America . . . . It was an absolute nightmare. It was ridiculous, absolutely ridiculous, that we’re in that circumstance.”

Family Members and Friends

HIPAA allows a health care provider to provide health information to an individual's family members and friends if:

- The provider has offered the individual an opportunity to object and the individual has not objected; or
- The individual is not available, and the Covered Entity, in its professional judgment, believes that the disclosure is in the best interests of the individual.

Family Members and Friends

- Health care providers may give patients the opportunity to identify those family members and friends to whom the patient would like information provided.
  - If designated family members or friends request verbal information about the patient, such information can generally be provided.
  - Unless the family member or friend has legal standing as a "personal representative" (defined on the next slide), the family member or friend is not typically permitted to receive written copies of the patient's records without the written authorization of the patient.

Personal Representatives

- A Personal Representative is an individual who is legally authorized to make decisions for the patient. When legally authorized, the Personal Representative "steps in the shoes" of the patient.
- This is usually an agent pursuant to a health care proxy or an individual holding a power of attorney.

Health Care Proxy

- The New York Health Care Proxy Law allows an individual to appoint someone — for example, a family member or close friend – to make health care decisions for that individual if he or she loses the ability to make decisions.
  - By appointing a health care agent, the individual can make sure that health care providers follow his or her wishes.
  - The Health Care Proxy typically does not have authority to make health care decisions unless the patient no longer is able to make his or her own health care decisions (*i.e.*, the patient is incapacitated).

Power of Attorney

- A power of attorney (or POA) is a legal document that gives one person (known as the "Agent") the authority to act for another person (known as the "Principal"). The POA form allows the Principal to specify exactly which decisions the Agent can make.
- The Agent does not have the authority to make health care decisions on behalf of the patient, but the POA is permitted to make decisions regarding payment, and therefore, can receive health care information in order to fulfill that responsibility.

Power of Attorney

GRANT OF AUTHORITY:

To grant your agent some or all of the authority below, either:

a) Initial the bracket at each authority you grant, or

b) Write or type the letters for each authority you grant on the blank line at (P), and initial the bracket at (P). If you initial (P), you do not need to initial the other lines.

I grant authority to my agent(s) with respect to the following subjects as defined in sections 5-1502A through 5-1502N of the New York General Obligations Law:

(____) (A) real estate transactions;

…….

(____) (K) health care billing and payment matters; records, reports and statements;

…….

(____) (P) EACH of the matters identified by the following letters:

A, B, C, D, E, F, G, H, I, J, K, L, M, N, and O

You need not initial the other lines if you initial line (P).

FAQ'S

If an individual with a POA or HCP is unable to provide the signed documents, and the notes in the health care provider's system reflect conversation with the POA/ HCP and confirmation that they have the POA/HCP, may the provider give *written* information to the person in the same manner as it would if the document had been on file?

No

If there is a patient who has appointed a POA or HCP, may the provider communicate with other family members? if so, which functions would have to be performed by the person with POA or HCP?

The provider can communicate with other family members if, in the professional judgment of its staff, the other family members need information to assist with care or payment for care.

FAQ'S

If the patient is cognitively intact and able to communicate, does the provider obtain information from the patient, or from the POA/HCP?

The provider should obtain information directly from the patient whenever possible. However, the provider may *obtain information from the POA or HCP as well as family members when appropriate.*

When does the POA/HCP become effective?

The POA becomes effective when signed but from a practical perspective it may be best to rely on the patient for release of information while the patient has capacity.

The HCP cannot make decisions, or receive health information, unless the patient is incapacitated.

FAQ'S

If a patient appoints a HCP, and the provider receives a request from a family member who is not the appointed HCP, does the provider have to verify with the HCP if the request should be processed?

No, the request can be processed.

Does a spouse override a Health Care Proxy?

No, not in regard to health care decisions.

FAQ'S

If there is a patient who has appointed a Power of Attorney, and a Health Care Proxy, who has more decision making power?

Once the patient is incapacitated, the HCP has the right to make health care decisions, the POA does not have the right to make health care decisions.

Can the POA authorize disclosure of patient information?

Yes, as long as the POA signs the authorization form.

Questions

THANK YOU!

Carmen E. Jule
Associate
Health Care/Compliance and White Collar Defense Practice Groups
516.393.2545
cjule@garfunkelwild.com

677 Broadway
7th Floor
Albany, NY 12207
(518) 242-7582

111 Great Neck Road
Suite 600
Great Neck, NY 11021
(516) 393-2200

350 Bedford Street
Suite 406A
Stamford, CT 06901
(203) 316-0483

411 Hackensack Ave.
5th Floor
Hackensack, NJ 07601
(201) 883-1030