Update on Data Privacy Enforcement Activity

HIPAA Privacy and Security Enforcement, plus more

KUTAKROCK

kutakrock.com

Presented by: Ruth S. Marcott, Esq.

August 2019

Legal Advice Disclaimer

- This presentation is for informational and discussion purposes only. This presentation is not intended to constitute legal advice and should not be relied on as such. You should always contact legal counsel prior to taking any actions related to any topics, issues, ideas, or suggestions discussed in this presentation.

Topics

- Overview – Privacy Rule and Security Rule
- HIPAA Audit Program
- HHS and FTC Enforcement
- Private Causes of Action Under State Privacy and Notification Laws
- State Data Security Laws
- Private Causes of Action Under State Data Security Laws
- Cybersecurity

Recent HHS Compliance Review

- Massachusetts General Hospital (“MGH”), Brigham and Women’s Hospital (“BWH”), and Boston Medical Center (“BMC”) recently paid a collective $999,000 penalty to HHS for breaching the Privacy Rule.

- The three hospitals allowed film crews from ABC to record in the hospitals for a medical documentary without obtaining the appropriate authorization from patients.

Recent HHS Compliance Review

Patient impact a worry with TV crews in Boston ERs

Filming of series in Boston hospitals stirs debate on balancing privacy concerns, public benefit

By Kay Lazar Globe Staff, January 12, 2015, 12:00 a.m.

Over four months, ABC News cameras had unparalleled access to three of Boston's renowned hospitals — Mass. General Hospital, Brigham and Women's Hospital, and Children's Hospital. (DONNA SVENNEVIK/ABC)

https://www.bostonglobe.com/metro/2015/01/12/debate-over-cameras-crew-films-boston/we50wuQ6bUPAU6sFcXA17H/story.html

Recent HHS Compliance Review

- HHS initiated the review after reading a news story posted on MGH's website and an article in the Boston Globe indicating ABC News would be filming a medical documentary at MGH, BWH and BMC.
- The hospitals provided the ABC film crews with the same HIPAA privacy training received by the workforces.
- HHS found the hospitals impermissibly disclosed PHI of patients to ABC employees during production and filming between October 2014 and January 2015.

Overview - Privacy Rule and Security Rule

Background

- HIPAA established national standards for the privacy and security of protected health information (“PHI”).
- The Health Information Technology for Economic and Clinical Health Act (“HITECH”) established breach notification requirements for individuals whose information may be at risk.
- The HHS Office for Civil Rights (“OCR”) helps assure compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

Privacy Rule

- The Privacy Rule deals with:
  - Notice of Privacy Practices;
  - Rights to request privacy protection of PHI;
  - Access of individuals to PHI;
  - Administrative requirements; and
  - Disclosures and uses of PHI.
- The Privacy Rule applies to all forms of PHI.

Breach Notification Rule

- The Breach Notification Rule applies to all forms of PHI.
- Top types of large breaches:
  - Theft;
  - Loss; and
  - Unauthorized access/disclosure.
- Most breaches are related to portable media.

Security Rule

- The Security Rule deals with:
  - Administrative safeguards;
  - Physical safeguards; and
  - Technical safeguards.
- The Security Rule applies only to electronic PHI.

Review of the Security Rule

- The Security Rule, officially titled “Security Standards for the Protection of Electronic Protected Health Information,” is Subpart C of Part 164 of Title 45 of the Code of Federal Regulations, 45 C.F.R. §§ 164.302-318.
- The major operative sections are Sections 306 (General Rules) 308 (Administrative Safeguards), 310 (Physical Safeguards), 312 (Technical Safeguards), and 314 (Organizational Requirements).

Enforcement Results by Year

- Outcome of Complaint Investigations

	Resolved After Intake and Review	Technical Assistance	Investigated: No Violation	Post-Investigational Technical Assistance	Investigated: Corrective Action Obtained	Total Resolutions
2015	12713	3817	360	188	542	17620
2016	16788	6201	204	231	476	23900
2017	15270	7307	253	219	668	23717
2018	16989	6912	267	289	632	25089

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#top

Enforcement Results by Year

- Outcome of Breach Compliance Review Investigations

	Resolved After: Intake and Review	Investigated: No Violation	Post-Investigational Technical Assistance	Investigated: Corrective Action Obtained	Other	Total Resolutions
2015	2	7	1	23	3	36
2016	1	3	0	10	1	15
2017	0	4	9	5	7	25
2018	0	2	1	4	0	7

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#top

Enforcement Results by Year

- Outcome of Other Compliance Review Investigations

	Resolved After: Intake and Review	Investigated: No Violation	Post-Investigational Technical Assistance	Investigated: Corrective Action Obtained	Other	Total Resolutions
2015	2	7	1	23	3	36
2016	1	3	0	10	1	15
2017	0	4	9	5	7	25
2018	0	2	1	4	0	7

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#top

Enforcement Results by Year

- Total Cases Investigated

	Investigated: No Violation	Post-Investigational: Technical Assistance	Investigated: Corrective Action Obtained	Total Investigated	Of Those, Settlements or CMPs	% of Total Investigated
2015	375	191	684	1250	6	0.48%
2016	232	257	743	1232	13	1.06%
2017	282	252	980	1514	10	0.66%
2018	284	331	995	1610	10	0.62%

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#top

Enforcement Results by Year

- Total Cases

	Complaints	Compliance Reviews	Technical Assistance	Total Cases	Of Those, Settlements or CMPs	% of Total Cases
2015	17620	176	4008	21804	6	0.0275%
2016	23900	334	6458	30692	13	0.0424%
2017	23717	396	7559	31672	10	0.0316%
2018	25089	438	7243	32770	10	0.0305%

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html#top

HIPAA Audit Program

HIPAA Audit Program

- In 2016 HIPAA began conducting random desk audits to monitor compliance with the Privacy and Security Rules.
- Audits review policies and procedures to assess adherence with the Privacy, Security, and Breach Notification Rules.

Privacy Audits

- Notice of Privacy Practices
  - Copy of all notices posted on the website and within the facility and notice distributed to individuals in places as of the end of the previous calendar year.
- Provision of Notice – Electronic Notice
  - URL for entity website and URL for posting of entity notice, if applicable.
  - Policies and procedures regarding provision of the notice electronically, if electronic notice is provided.
  - Documentation of an agreement with the individual to receive the notice electronically.

Privacy Audits

- Right to Access
  - Policies and procedures for individuals to request access to PHI.
  - All documentation related to the first five access requests which were granted and evidence of fulfillment in the previous calendar year.
  - All documentation related to the last five access requests for which the entity extended the time for response to the request.
  - Any standard template or form letter required or used by the covered entity (“CE”) to document access requests.

Security Audits

- Risk Analysis
  - Policies and procedures regarding entity's risk analysis process.
  - Documentation demonstrating that policies and procedures were in place and in force six years prior to the date of receipt of notification.
  - Documentation from the previous calendar year demonstrating the policies and procedures are available to the persons responsible for implementing the risk analysis and that such documentation is periodically reviewed and updated, if needed.
  - Documentation of the current risk analysis and the most recently conducted prior risk analysis.
  - Documentation of current risk analysis results.

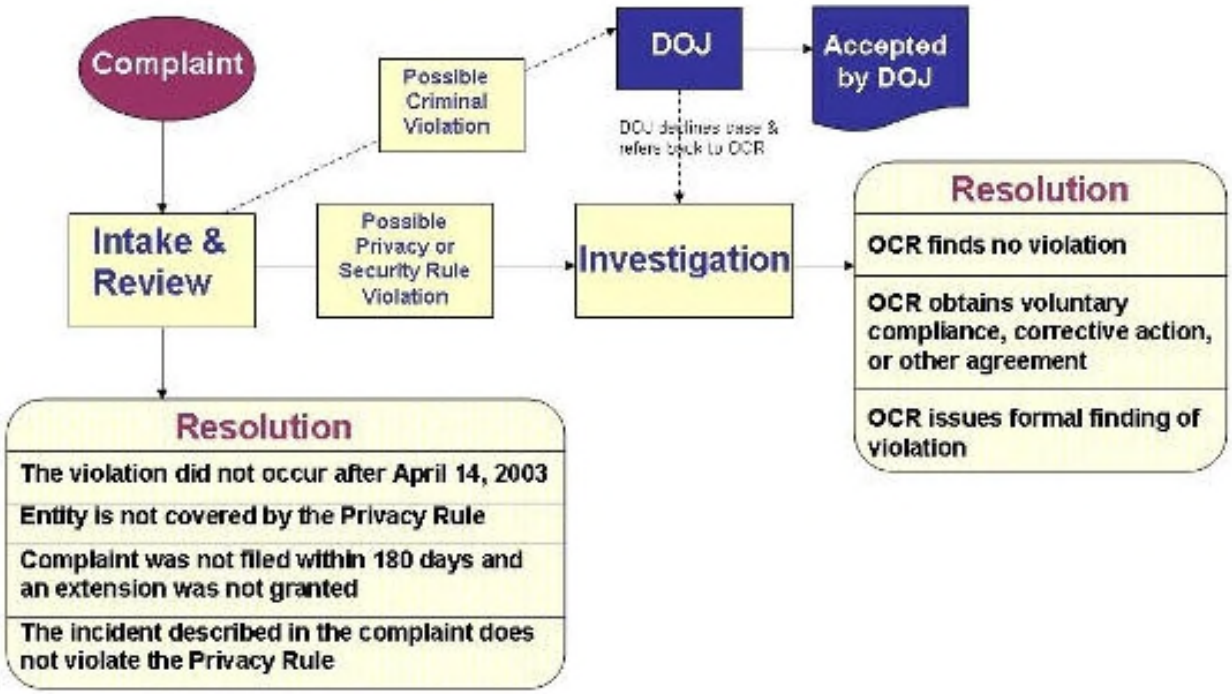
Security Audits

- Risk Management
  - Policies and procedures related to the risk management process.
  - Documentation demonstrating that policies and procedures related to the implementation of risk management were in place and in force six years prior to the date of receipt of the notification.
  - Documentation demonstrating the policies and procedures are available for the persons responsible for implementing them and that such documentation is periodically reviewed and updated, if needed.
  - Documentation demonstrating the efforts used to manage risks from the previous calendar year.
  - Documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment .

Breach Audits

- Timeliness of Notification
  - Documentation of five breach incidents for the previous calendar year affecting fewer than 500 individuals, documenting the date the individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification.
- Content of Notification
  - Documentation of five breach incidents affecting 500 or more individuals for the previous calendar year.
  - A copy of a single written notice sent to affected individuals for each breach incident.
  - If the entity used a standard template or form letter, a copy of the document.

HIPAA Privacy & Security Rule Complaint Process



https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html

KUTAKROCK

HHS Enforcement Actions and Settlement Agreements

Complaint Focus Areas

- General hospitals
- Private practices and physicians
- Outpatient facilities
- Pharmacies
- Health Plans (group health plans and health insurance issuers)
- Business Associates

Common Trends in HHS Enforcement Actions

- Failure to implement policies and procedures.
- Failure to implement a mechanism to encrypt and decrypt ePHI when it was reasonable and appropriate to do so under the circumstances.
- Failure to sign a Business Associate Agreement (“BAA”) or require a BAA.
- Corrective Action Plans (“CAPs”) and fines.

Top Five Issues Investigated in Cases Closed with a Corrective Action, 2015-2018

1. Impermissible Uses and Disclosures
2. Safeguards
   - Physical measures, policies, and procedures to protect a CE's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.
3. Administrative Safeguards
   - Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the CE's workforce in relation to the protection of that information.
4. Access
5. Technical Safeguards
   - The technology and the policies and procedures and its use that protect ePHI and control access to it.

Touchstone Medical Imaging ("TMI")

An insecure file transfer protocol ("FTP") resulted in the public exposure of 307,839 individuals' names, dates of birth, phone numbers, addresses, and some social security numbers; the FTP server was configured to allow anonymous connections to a shared directory.

Touchstone Medical Imaging ("TMI")

HHS found that TMI:

- **Failed to implement technical policies** and procedures to allow access only to those persons or software programs that have been granted rights to an FTP server that maintained ePHI until May 9, 2014;
- **Failed to enter into a written BAA** with its business associate MedIT Associates;
- Continued to engage business associate XO Communications **without a BAA** in place;
- **Failed to conduct an accurate and thorough assessment** of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by it;
- **Over a 4-month period**, **failed to accurately identify** and respond to a known security incident, **mitigate** the harmful effects (to the extent practicable), and **document** the security incident and its outcome, and **failed to notify** individuals and media outlets until 147 days from the date the breach was discovered.

Key Terms of TMI's Settlement Agreement/CAP

- Conduct a complete and accurate, thorough, enterprise-wide analysis of security risks and vulnerabilities that incorporates all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by TMI or its affiliates that are owned, controlled, or managed by TMI that contain, store, transmit, or receive TMI ePHI.
- Develop a complete inventory of all electronic equipment, data systems, off-site data storage facilities, and applications that contain or store ePHI.
- Develop an organization-wide risk management plan to address and mitigate any security risks and vulnerabilities identified in its risk analysis.

Key Terms of TMI's Settlement Agreement/CAP

- Annually conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by TMI, affiliates that are owned, controlled, or managed by TMI.
- Review and revise written policies and procedures to comply with the Privacy, Security, and Breach Notification Rules.
- Submit annual reports to HHS with respect to the status of and findings regarding its compliance with the CAP.

Key Terms of TMI's Settlement Agreement/CAP

- Revise its BAA policies and procedures to:
  - Designate one or more individual(s) responsible for ensuring TMI enters into a BAA with each of its business associates;
  - Create a process for assessing current and future business relationships to determine whether each relationship is with a "business associate;"
  - Create a process for negotiating and entering into BAAs with business associates prior to disclosing PHI to the business associate;
  - Create a standard template BAA;
  - Create a process for maintaining documentation of a BAA for at least six years beyond the date when the business associate relationship is terminated; and
  - Limit disclosures of PHI to business associates to the minimum necessary amount of PHI that is reasonably necessary for business associates to perform their duties.

2018 Settlement Agreements and Judgments

Name	Violation	Penalty
Filefax, Inc.	Impermissible disclosure of PHI by leaving PHI in an unlocked truck (settlement).	$100,000
Fresenius Medical Care North America	Five separate breach incidents over a five month period implicating ePHI of five Fresenius-owned CEs (settlement).	$3,500,000
MD Anderson	Theft of unencrypted laptop and two unencrypted USB thumb drives containing unencrypted ePHI of over 33,500 individuals (judgment).	$4,348,000
Advanced Care Hospitalists	Patient information viewable on medical billing services' website; did not have BAA with the individual providing medical billing services (settlement).	$500,000
Allergy Associates of Hartford	Doctor impermissibly disclosed patient PHI to a reporter (settlement).	$125,000

2018 Settlement Agreements and Judgments

Name	Violation	Penalty
Anthem, Inc.	Series of cyberattacks that led to the largest U.S. health data breach in history. Cyber attackers infiltrated the system through phishing emails that at least one employee responded to, opening the door to further attacks. Almost 79 million individuals impacted (settlement).	$16,000,000
Pagosa Springs	Former employee continued to have access to web-based scheduling calendar, which contained ePHI, after separation of employment, resulting in impermissible disclosure of ePHI of 557 individuals (settlement).	$111,400
Cottage Health	Two breaches of unsecured ePHI affecting over 62,500 individuals (settlement).	$3,000,000

Penalty Caps

- OCR announced on April 30, 2019 that it is lowering the maximum total penalties it may assess against covered entities and business associates for multiple violations of a single HIPAA provision in a single calendar year.
- Covered entities and business associates that demonstrate that any violations were **due to lack of knowledge** or to **reasonable cause** and take action to correct any violations within 30 days may qualify for significantly lower annual caps on penalties.
- Previously the maximum penalty for a violation was $1.7M in a single year; **the cap is being lowered to $28,526 per year, a 6,000% decrease.**

Federal Trade Commission ("FTC") Enforcement

Division of Privacy and Identity Protection

Benchmarks for Data Security

The Eleventh Circuit's opinion in *LabMD v. FTC* highlighted the FTC's specific benchmarks for data security, replacing the former "reasonableness" standard, including:

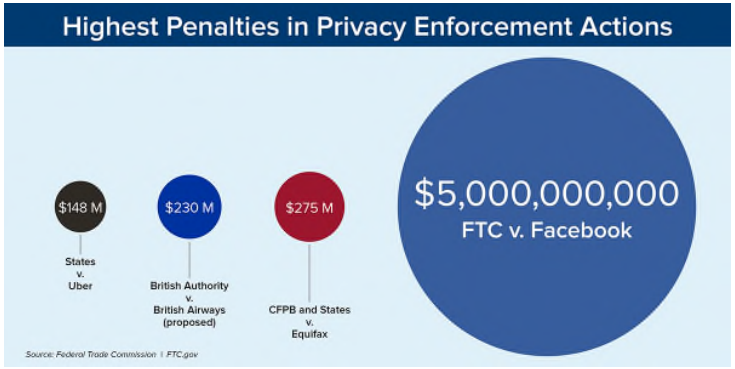
- Using suitable risk-assessment tools;
- Providing data security training to employees; and
- Adequately restricting and monitoring the computer practices of those using the network.

Going forward, the FTC is expected to shift to more customized conditions for companies who fail to properly handle consumer data.

$5B Facebook Settlement

- Facebook violated a 2012 FTC order regarding previous privacy-related violations.
- Among the violations included the failure of Facebook to adequately assess and address privacy risks posed by third-party developers; Facebook did not screen the developers or their apps before giving them access to massive amounts of data that Facebook users designated as private.

$5B Facebook Settlement



- Facebook is now required to implement a stringent program **to monitor third-party developers and terminate access to any developer** that doesn't follow the rules.
- Facebook must also implement a comprehensive data security program. Expert compliance officers will be responsible for documenting every material privacy decision in detail.

https://www.impactbnd.com/blog/ftc-slaps-facebook-with-5-billion-penalty

Private Causes of Action Under State Privacy and Notification Laws

Menorah Park Center for Senior Living v. Rolston, 2019 WL 2303146 (2019) (Ohio)

- Rehab therapy facility filed a small claims complaint against a former patient to recover a debt related to health care services and included an unredacted copy of account billing statements that included a description of medical services with the complaint.
- The court recognized that HIPAA allows the disclosure of minimum information necessary to obtain payment for health care services, **but a copy of medical bills or other detailed evidence is *not required* for collection on a debt.**

Menorah Park Center for Senior Living v. Rolston, 2019 WL 2303146 (2019) (Ohio)

- The court held that **an independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information** that a physician or hospital has learned within a physician-patient relationship.

Byrne v. Avery Center for Obstetrics and Gynecology, P.C., 327 Conn. 540 (2018)

- Avery Center for Obstetrics and Gynecology mailed a copy of plaintiff's medical file to the court in response to a subpoena; the medical file was not sealed and a third party who was bringing a paternity claim against the plaintiff was able to view the records.
- The court held that the most common basis for recognizing a cause of action for breach of confidentiality of medical records by health care providers is that **health care providers enjoy a special fiduciary relationship** with their patients and recognition of the privilege is necessary to ensure the bond remains.

Byrne v. Avery Center for Obstetrics and Gynecology, P.C., 327 Conn. 540 (2018)

- The court also held that the duty of confidentiality arises from the physician-patient relationship and the unauthorized disclosure of confidential information obtained in the course of that relationship for the purpose of treatment gives rise to a cause of action sounding in tort against the health care provider, unless the disclosure is otherwise allowed by law.

State Data Security Laws

State Data Security Laws

- At least 25 states have laws that address data security practices of private sector entities. Most data security laws require businesses that own, license, or maintain personal information about a resident of that state to implement and maintain “reasonable security procedures and practices” appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Ohio

- Law applies to any business or nonprofit entity, including a financial institution, that accesses, maintains, communicates, or handles personal information or restricted information.
- **To qualify for an affirmative defense** to a cause of action alleging a failure to implement reasonable information security controls resulting in a data breach, an entity must create, maintain, and comply with a **written cybersecurity program** that contains administrative, technical, and physical safeguards for the protection of personal information as specified (e.g., conforming to an industry recognized cybersecurity framework as listed in the act).
- Ohio Rev. Stat. § 1354.01 to 1354.05 (2018 S.B. 220).

Massachusetts

- Law applies to any person that owns or licenses personal information.
- Authorizes regulations to ensure the security and confidentiality of customer information in a manner fully consistent with industry standards. The regulations shall take into account the person's size, scope, and type of business, resources available, amount of stored data, and the need for security and confidentiality of both consumer and employee information.
- Mass. Gen. Laws Ch. 93H § 2(a)

California Consumer Privacy Act ("CCPA") – Effective January 1, 2020

- Provides rights to Consumers regarding their personal information; a **Consumer is a natural person who is a California resident.**
- Defines "Personal Information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." **Personal Information originates from a Consumer**.
- The CCPA excludes certain types of information that would otherwise meet the definition of Personal Information, including information regulated by HIPAA.

California Consumer Privacy Act ("CCPA") – Effective January 1, 2020

- **Consumer rights** include disclosure/privacy policy requirements, access/data portability, deletion, and opt out requirements/non-discrimination.
- Imposes burdens on businesses, service providers, and third parties.
- Will be enforced by the CA Attorney General, who will have the authority to bring an action for up to $2,500 for any violation of the CCPA; damages are calculated on a per-capita basis.
- Provides a private right of action for Consumers.

Private Causes of Action Under State Data Security Laws

Cassell v. Vanderbilt University, 285 F.Supp.3d 1056 (M.D. Tenn. 2018)

- Defined contribution participants brought a breach of fiduciary duty claim against employer-sponsor Vanderbilt University for breaching its duties of loyalty and prudence and by locking the Plan into unreasonable administrative fees, unreasonable management, and engaging in prohibited transactions.
- The court dismissed the breach of loyalty claim but found that the plaintiffs could move forward with the breach of the duty of prudence.

Cassell v. Vanderbilt University, 285 F.Supp.3d 1056 (M.D. Tenn. 2018)

- The plaintiffs then amended their complaint to claim the defendants **breached their duty to participants** by allowing the **Plan's record-keeper to obtain access to participants, gaining valuable, private, and sensitive information** including participants' contact information, their choices of investments, the asset sizes of their accounts, their employment status, age, and proximity to retirement, among other things. They claimed defendants allowed the record-keeper to use this information to sell the record-keeper's products and wealth management services to the Plan's participants and failed to attempt to determine the value of the marketing benefit.

Cassell v. Vanderbilt University, 285 F.Supp.3d 1056 (M.D. Tenn. 2018)

- Defendants were aware of the record-keeper's misuse of the information and did nothing to prevent the misuse. Defendant also failed to establish safeguards to prevent such misuse from occurring.
- The parties ultimately settled with Vanderbilt paying $14.5 million to settle all the allegations.

Divane v. Northwestern Univ., No. 16 C 8157 (N.D. Ill May 25, 2018)

- Participants sued plan sponsor arguing the plan had too many options, excess fees, and that the plans allowed the record-keeper to market product to the participants.
- The court concluded that **confidential information is not a plan asset** because it is not property "under the ordinary notions of property rights," and that the participants did not cite a case in which a court held that releasing confidential information or allowing someone to use confidential information constitutes a breach of fiduciary duty under ERISA.

Additional Civil Remedies

- The HITECH Act gave state **Attorneys General** the power to file civil actions on behalf of state residents for violations of HIPAA Privacy and Security Rules. State Attorneys General are also permitted to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy/Security Rules.

Cybersecurity

Cybersecurity

- The ERISA Advisory Council 2016 Report on Cybersecurity recommends cybersecurity discussions include:
  - What and how data is held
  - Different ways to access the data
  - How the data is transferred
  - Where the data is transferred
  - Whether unrelated parties can disrupt the data flow

Cybersecurity

- Encryption should be an essential component of cybersecurity strategy, particularly where data is transferred among multiple parties or companies.
- The Society of Professional Asset-Managers and Recordkeepers ("SPARK") is in the process of establishing uniform data management standards for the defined contribution retirement plan market.

Cybersecurity

- The Health Information Trust Alliance ("HITRUST") is a not-for-profit consortium that represents various providers in the healthcare industry with regard to cybersecurity and works to raise the level of security within the industry. HITRUST developed a Common Security Framework ("CSF"), tools, and cyber Risk Management Framework ("RMF").
- HITRUST CSF and RMF are free.

Summary

- HHS continues to investigate and enforce HIPAA privacy and security issues vigorously.
- State law, common law, FTC rules and other regulations further regulate PHI and other private data.
- Cybersecurity best practices are evolving and require constant review.

(DONNA SVENNEVIK/ABC)

Questions?

Ruth S. Marcott, Esq.
Kaitlin D. Riessen, Esq.
Kutak Rock LLP
60 S. Sixth Street, Suite 3400
Minneapolis, MN 55402
612-334-5044
Ruth.Marcott@KutakRock.com

KUTAKROCK