OCR Audits: Past, Present, and Future Considerations for Privacy and Security

Edye T. Edens, JD, MA, CIP, CCRP
Deanna Peterson, MHA, RHIA, CHPS, LNHA

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

1

What we are doing today

- Discuss HIPAA do's and don't's for research
- Review OCR enforcement and current state of audits
- Discuss recent HIPAA waivers related to COVID-19 and impact on research

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

2

HIPAA Basics

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

3

HIPAA Identifiers

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes
- All elements of dates (except year); and all ages over 89 and all elements of dates (including year) may be aggregated into a single category of age 90 or older
- Telephone numbers
- Facsimile numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers.
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images
- Any other unique identifying numbers, characteristics, or codes

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

4

Use of PHI

Under HIPAA, PHI may be accessed without an authorization if used for TPO:

- ***T*** Treatment
- ***P*** Payment
- ***O*** Health care Operations

Research activities are NOT part of TPO

If not TPO, patient authorization or exception

5

Minimum Necessary

- HIPAA requires that use of, disclosure of and requests for PHI be limited to the ***minimum necessary*** to accomplish the intended goal or purpose
  - Only access, use, or disclose the PHI necessary to accomplish the task and only for a business need
- Requests for and use of PHI must be limited to the minimum necessary to conduct that research, unless the subject provides specific Authorization regarding use of the data

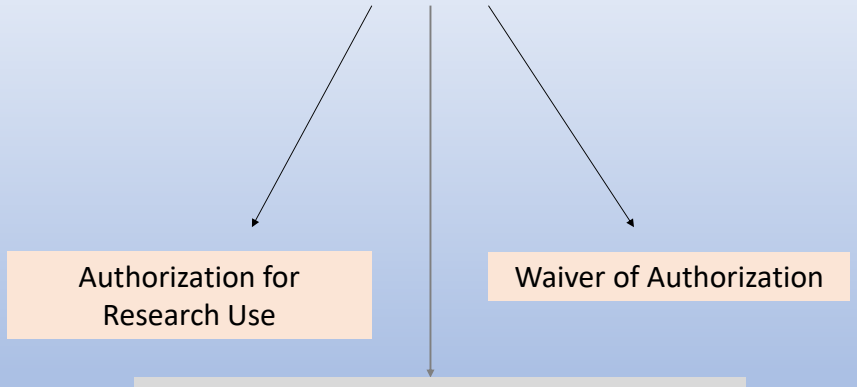
6

Authorization

FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

7

Use of PHI for Research



FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

8

Authorization for Research

- **Authorization Core Elements** (see Privacy Rule, *45 C.F.R.* §164.508(c)(1))
- Description of PHI to be used or disclosed (identifying the information in a specific and meaningful manner).
- The name(s) or other specific identification of person(s) or class of persons authorized to make the requested use or disclosure.
- The name(s) or other specific identification of the person(s) or class of persons who may use the PHI or to whom the covered entity may make the requested disclosure.
- Description of each purpose of the requested use or disclosure. Researchers should note that this element must be research study specific, not for future unspecified research.
- Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure (the terms "end of the research study" or "none" may be used for research, including for the creation and maintenance of a research database or repository).
- Signature of the individual and date. If the Authorization is signed by an individual's personal representative, a description of the representative's authority to act for the individual.
- **Authorization Required Statements** (see Privacy Rule, *45 C.F.R.* § 164.508(c)(2))The individual's right to revoke his/her Authorization in writing and either (1) the exceptions to the right to revoke and a description of how the individual may revoke Authorization or (2) reference to the corresponding section(s) of the covered entity's Notice of Privacy Practices.
- Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization.
- The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health information.*

FCS FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

9

Authorization for Research: Special Considerations

- May state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the “end of the research study”
- May be combined with a consent to participate in the research, or with any other legal permission related to the research study
- May be combined with an authorization for a different research activity, provided that, if research-related treatment is conditioned on the provision of one of the authorizations, such as in the context of a clinical trial, then the compound authorization must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the unconditioned research activity
- May be obtained from an individual for uses and disclosures of protected health information for future research purposes, so long as the authorization adequately describes the future research such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for the future research purposes

FCS FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

10

Guidance for HIPAA Authorizations for Future Use

- Description of Purpose
- Expiration
- Right to Revoke

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

11

Accounting of Disclosures

- Need to account only outside of your "workforce"
  - Outside the CE unless recipient is designated as a "workforce member"
  - Log
- Exceptions
  - Implied/internal workforce
    - Could also be to subject of the PHI, OR
    - For treatment, payment, QA/QI, auditing purposes
  - Authorization executed naming outside researcher
  - Disclosure contains only "indirect Identifiers" permitted in a HIPAA Limited Data Set
- Tracking
  - What exactly was disclosed and to exactly whom
  - Why – mandated? Research? Was a waiver involved?
  - How – often organization specific

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

12

Waivers

FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

13

Waiver of Authorization

- Privacy Board can approve requests for waiver of authorization for research purposes
- Allows the Privacy Board to stand in the shoes of the patient
- IRB can serve as the Privacy Board

FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

14

Waiver of Authorization Documentation

- Identification of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
- A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the three criteria in the Rule;
- A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or Privacy Board;
- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
- The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

15

Waiver of Authorization Criteria

1. The use or disclosure involves no more than minimal risk to the privacy of individuals based on:
   a. An adequate **plan to protect** the identifiers from improper use/disclosure
   b. An adequate **plan to destroy** the identifiers at the earliest opportunity
   c. Adequate **written assurances** that the PHI will not be reused/disclosed to any other person or entity, with certain exceptions

16

Waiver of Authorization Criteria

2. The research could not practicably be conducted without the waiver
3. The research could not practicably be conducted without access to and use of the PHI

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

17

Practicability

- Feasibility
  - Capable of being effected, done, or put into practice
  - May be practiced or performed
  - Capable of being done or accomplished with available means or resources
- Issue: practicability of performing the research
  - NOT practicability of obtaining authorization

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

18

Practicability

Scientific validity	Ethical concerns	Pragmatic concerns
• Sample size required is so large that including only those from whom authorization would be obtained would bias the results • Subjects are no longer seen and/or lost to follow up • Too many subjects to contact	• Additional threats to privacy from the link between authorization and data • Risk of inflicting psychological, social, or other harm by contacting individuals and/or families (e.g. subjects are gravely ill or a child has died)	• Subjects seen at too many sites to cover • Subjects seen at times which are not practicable • Inability to identify subjects beforehand • Too many subjects

FCS FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

19

Exceptions

FCS FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

20

Reviews Preparatory to Research

- The use or disclosure of PHI is sought solely to prepare a protocol or a similar preparatory purpose;
- PHI will not be removed from the covered entity; *and*
- PHI is necessary for research purposes

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

21

Decedents' Information

- Use or disclosure solely for research on decedents' information;
- PHI is necessary for research; and
- Individual is a decedent, and provide documentation upon covered entity's request

NOTE: Under the HITECH Act, HIPAA only protects an individual's information until 50 years after date of death

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

22

De-identified Data

- Safe Harbor Method: 18 identifiers removed from data and no knowledge that remaining information can (alone or in combination with other information) identify the individual.

  or

- Statistically "de-identified" information. A qualified statistician determines that there is a "very small" risk that the information could be used, alone or in combination with other reasonably available information, to identify the individual and documents the methods and results of the analysis

23

Limited Data Set

- Limited Data Set may be released without authorization
- Requires a data use agreement between the covered entity and the recipient
- The Limited Data Set can contain:
  - Elements of Dates;
  - City, town, state, and ZIP;
  - Other unique identifiers, characteristics and codes not previously listed as direct identifiers

24

Other Exceptions

- Disclosures required by law
- Disclosures to public health authorities
- Disclosures for adverse event reporting to certain persons subject to the jurisdiction of the FDA

25

OCR Enforcement

26

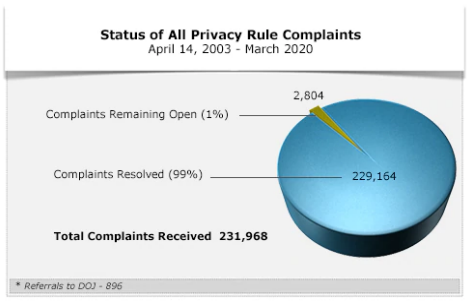
OCR Enforcement

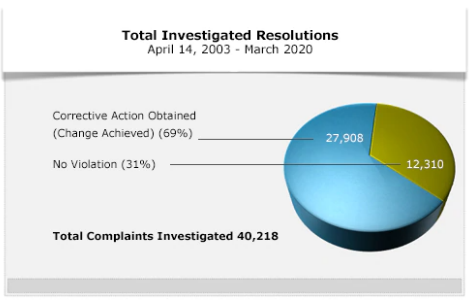
- Federal civil rights laws, conscience and religious freedom laws, the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule
- Enforcement: Teach, Educate and Investigate

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

27

Complaints





75 cases resolved with CMPs totaling $116,303,582.00

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

28

Complaints

FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

29

Complaint Intake

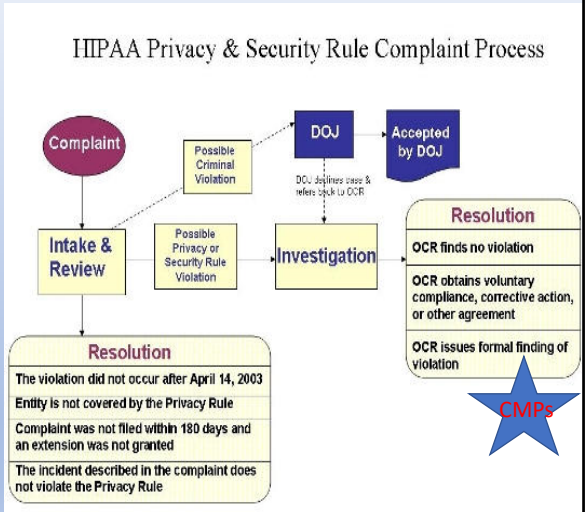
- Action took place after security and privacy rule were in effect
- Involve a covered entity
- Violation of privacy or security rule
- Filed within 180 days*

FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

30

OCR Complaint Process

1. **Resolved after intake**
2. **Technical assistance**
3. **No violation (investigated)**
4. **Corrective action (investigated)**
5. **Other**



31

Civil Money Penalties

Penalty Tier	Level of Culpability	Minimum Penalty per Violation (2018 » 2019)	Maximum Penalty per Violation (2018 » 2019)	New Maximum Annual Penalty (2018 » 2019)*
1	No Knowledge	**$117**	**$58,490**	**$25,630**
2	Reasonable Cause	**$1,170**	**$58,490**	**$102,522**
3	Willful Neglect – Corrective Action Taken Within 30 Days	**$11,698**	**$58,490**	**$256,305**
4	Willful Neglect – No Timely Corrective Action Taken	**$58,490**	**$1,754,698**	**$1,754,698**

32

Criminal Penalties

- Knowingly obtain or disclose PHI: up to $50k + 1 year imprisonment
- False pretenses: $100k + 5 years imprisonment
- Intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm: $250k + 10 years imprisonment

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

33

OCR Enforcement

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2019	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2018	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safegards
2017	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2016	Access	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Technical Safeguards

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

34

Settlements

35

Feinstein Institute for Medical Research

- 3/17/16 – Settled for $3.9 million
  - Unsecured laptop stolen with approximately 13,000 patients and research participants
- What they found:
  - Failure to conduct sufficient risk analysis
  - Failure to implement and follow policies and procedures
  - Failure to implement safeguards

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

36

Children's Medical Center of Dallas

- **2/1/17** - OCR announced a CMP against Children's for **$3.2** million
  - 2009 lost unencrypted blackberry device with 3,800 patients
  - 2013 stolen unencrypted laptop with 2,462 patients
- What they found:
  - Failing to implement risks management plans
  - Failing to deploy encryption or an equivalent measure
  - Lack of timely action
- https://www.hhs.gov/about/news/2017/02/01/lack-timely-action-risks-security-and-costs-money.html

FCS First Class Solutions, Inc℠ Not Your Traditional Healthcare Consulting Firm ...

37

Memorial Healthcare System

- **2/16/17** - OCR announced a settlement with Memorial Healthcare Systems for **$5.5** million
  - Impermissible disclosure of 115,143 patients
  - Login of former employee
  - Breach occurred continuously from 2011-2012
- What they found:
  - Failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access
  - Lack of audit controls
  - Failed to follow through on risk analysis deficiencies
- Lack of access control
- https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html

FCS First Class Solutions, Inc℠ Not Your Traditional Healthcare Consulting Firm ...

38

Memorial Hermann Health System (MHHS)

- **5/10/2017** - OCR announced MHHS settled for **$2.4** million
  - Press release without authorization
- What they found:
  - Improper disclosure

- https://www.hhs.gov/about/news/2017/05/10/texas-health-system-settles-potential-hipaa-disclosure-violations.html

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

39

Enforcement Takeaways

- Thorough risk analysis
  - Address opportunities identified
- Appropriate policies and procedures
  - And follow them!
- Ongoing education
  - Customized to research

FCS First Class Solutions, Inc℠
Not Your Traditional Healthcare Consulting Firm ...

40

COVID-19

41

COVID-19 Considerations

- Tied to nationwide/state public health emergency
- Check your state for waivers/guidance
- Several waivers, guidance and enforcement discretion from HHS
  - Media
  - Testing sites
  - BAAs
  - Apps for telehealth
    - Do NOT use Facebook Live, Twitch, TikTok, and similar video communication applications
  - First responders – release of addresses
  - Sharing information
- https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html

42

COVID-19 Considerations

- Documentation of pivots
  - Retention of emails
    - Note to file
- Remote consent
- Remote monitoring and source data verification
- Telehealth consent and modalities
  - HHS list

43

Questions?

44

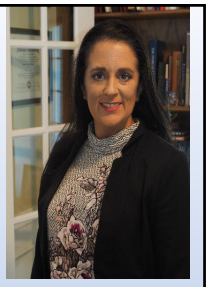
Deanna Peterson, MHA, RHIA, CHPS, LNHA
Vice President, Health Information Consulting Services
Deanna.Peterson@FirstClassSolutions.com

Deanna serves at the Vice President for Health Information Management Services and Privacy Officer for the firm. She conducts Operational Assessments, serves in HIM Interim Management positions, and provides ongoing guidance on operations, compliance and regulatory issues, privacy, LHR, and EHR selection for a variety of settings. She established the LTC service line that serves close to 100 facilities in multiple states.

Ms. Peterson received her B.S. in Health Information Management and M.H.A. from Saint Louis University. She is an active member of the Missouri Health Information Management Association (MoHIMA) currently serving as President, and the American Health Information Management Association (AHIMA) currently serving as Co-Chair of the Long Term Post-Acute Care Practice Council. She received the 2016 Outstanding Volunteer Award from MoHIMA and 2017 Emerging Leader Award from AHIMA.

FCS FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

45



Edye T. Edens, JD, MA, CIP, CCRP
Senior Research Compliance Consultant

Joining First Class Solutions, Inc. in 2017, Edye T. Edens serves as our Senior Research Compliance Consultant focusing on research compliance and life sciences. Edye is a licensed attorney with an international human rights, research ethics, and health law background.

Her consulting services include research administration, healthcare compliance, grants/contracts to IRB, COI, education, privacy,
HIPAA, multiple areas of FDA compliance related to drugs, devices, and food; AAHRPP, misconduct and site-level compliance work as it relates to QA, monitoring, and auditing (particularly oncology). Services provided include education and training, program creation and management, or even as a complete outsourcing solution. Additionally, Ms. Edens regularly publishes articles and speaks at regional and national professional research and compliance association meetings, including HCCA, SCCE, PRIM&R, MAGI, AAHRPP, SPARC, RAPS, and AHLA.

Previously, while in-house for a decade at Indiana University, she focused on the role of human rights in health and worked at the Human Subject Offices on both the Bloomington and Indianapolis campuses, the Indianapolis Grant Services office, Clinical Research Compliance Office and the Research Integrity Office aiding in quality assurance and compliance matters including managing accreditations, internal auditing, education and managing consultation projects involving outside entities. In 2016, she became the first Quality and Compliance Manager for the IU Simon Cancer Center over all aspects of compliance related to all clinical trials performed at IUSCC, before departing for the consulting world.

Educationally, she completed her MA in International Research Ethics in 2012, and was the program manager for a NIH grant to aid in creating a joint international institutional review board (IRB) in conjunction with IU's existing Moi University medical school partnership in Kenya and the IU Center for Bioethics. She is also a Certified IRB Professional (CIP), Certified Clinical Research Professional (CCRP), and holds a green belt certification in Lean Six Sigma. Additionally, she teaches at IU's McKinney School of Law in Indianapolis, and oversees the Hall Center for Law and Health's Externship Program.

FCS FIRST CLASS SOLUTIONS, INC℠
Not Your Traditional Healthcare Consulting Firm ...

46