# Operationalizing Government Corrective Action Plans: Aftermath of an OCR Investigation

Presented By:

Emmelyn Kim, MA, MPH, CCRA, CHRC
AVP, Research Compliance & Privacy Officer &

Kathleen McGill, MPA, CTR, CPHQ, CIP
VP, Administrative Operations

The Feinstein Institute for Medical Research

Northwell Health℠

1

**Emmelyn Kim** is AVP, Research Compliance & Privacy Officer at the Feinstein Institute for Medical Research, Northwell Health. She oversees the research compliance programs including quality assurance, regulatory affairs, export controls and conflict of interest. This includes audits and investigations pertaining to HIPAA, allegations of research non-compliance or misconduct. She reports to the Chief Corporate Compliance Officer and the Board's Executive Audit and Corporate Compliance Committee.

**Kathleen McGill** is VP, Administrative Operations at the Feinstein Institute for Medical Research, Northwell Health. She oversees the day to day operations of a large multi-faceted research service line. Kathleen reports to the Chief Medical Officer & Senior Vice President.

***Disclaimer***

***The materials and view expressed in this presentation are the views of the presenters and not necessarily the views of Northwell Health***

Northwell Health℠

2

## Audience Ice Breaker & Polling

## A Quick Recap

## Learning Objectives

1. Discuss key components of carrying out a Corrective Action Plan (CAP): People, Planning and Process
2. Consider unanticipated government challenges, external resources and cost
3. Discover what complex organizations should consider in their training programs

## Discuss key components of carrying out a Corrective Action Plan (CAP): People, Planning and Process

## Elements of an Office for Civil Rights (OCR) CAP

Security Management Process

- Risk analysis

## Elements of an Office for Civil Rights (OCR) CAP

Implementation of Process for Evaluating Environmental and Operational Changes

- Standard Operating Procedure (SOPs)

# Elements of a CAP (continued)

Policies and Procedures (P&Ps)

- Distribution and Updating P&Ps
- Minimum Content
- Certifications

Minimum content:

- Uses and Disclosures of PHI [45CFR§164.502(a)]
- Security Management Process [45CFR§164.308(a)(1)(i)]
- Information Access Management [45CFR§164.308(a)(4)]
- Workstation Security [45CFR§164.310(c)]
- Device and Media Controls [45CFR§164.310(d)]
- Encryption and Decryption [45CFR§164.312(a)(2)(iv) & 164.312(e)(2)(ii)]

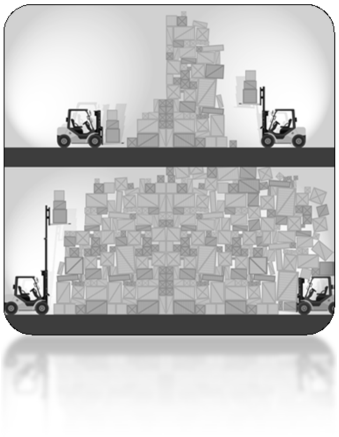
# Elements of a CAP (continued)

Health Information Portability and Accountability Act (HIPAA) Training for Workforce

- Certifications
- Tracking existing and new hires

# Reporting & Other Requirements

1. Reportable Events
2. Implementation Report
3. Annual Reports
4. Document Retention
5. Breach Provisions



# People

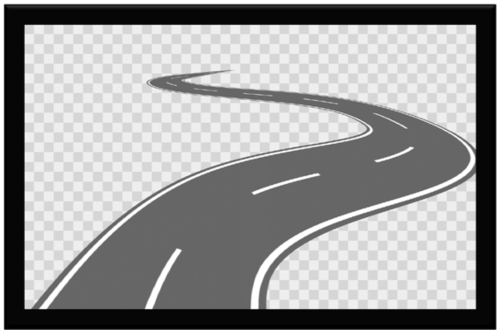
Our workgroup included senior representatives with ***decision making authority*** from:

- Organizational Leadership
- Administration/Operations
- Compliance
- Legal
- IT Security/Risk Management
- Public Relations
- Human Resources
- Policy and Training

*The workgroup may include others and will evolve over time*

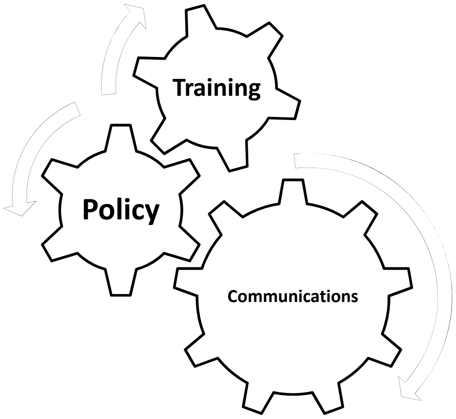
# Planning

- Developing a timeline for the CAP
- Regularly occurring touch points/meetings
- Setting expectations
- Communications



# Processes

- Establish smaller working groups to evaluate and develop processes
- Connection to larger organizational Committees



## Consider unanticipated government challenges, external resources and cost

## Things to Think About

Compliance

- Contact, reporting progress & issues
- Tracking and reporting to OCR
- Reporting upwards

# Things to Think About

Legal:

- Dedicated internal legal counsel
- Outside counsel with OCR experience
- Response strategy and time frames

# Things to Think About

Operational:

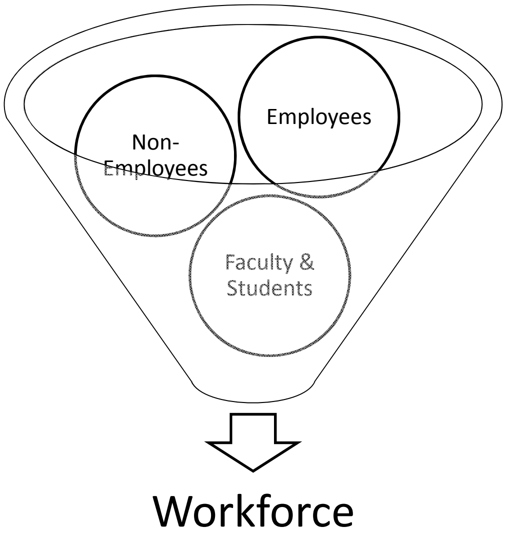
- Administration
- Developing processes

→ *Think about hiring a Project Manager*

# Who is Your Workforce?

Operational:

- Tracking workforce
- Communications
- Reporting to Compliance



Northwell Health

# Things to Think About

IT Security

- Risk Assessments & timeframes
- Vendors
- Costs

Northwell Health

## Things to Think About

Education and Training:

- Electronic vs. in-person
- Pilot testing
- Tracking and reporting
- HR and escalation procedures

## When you thought you got it all covered…

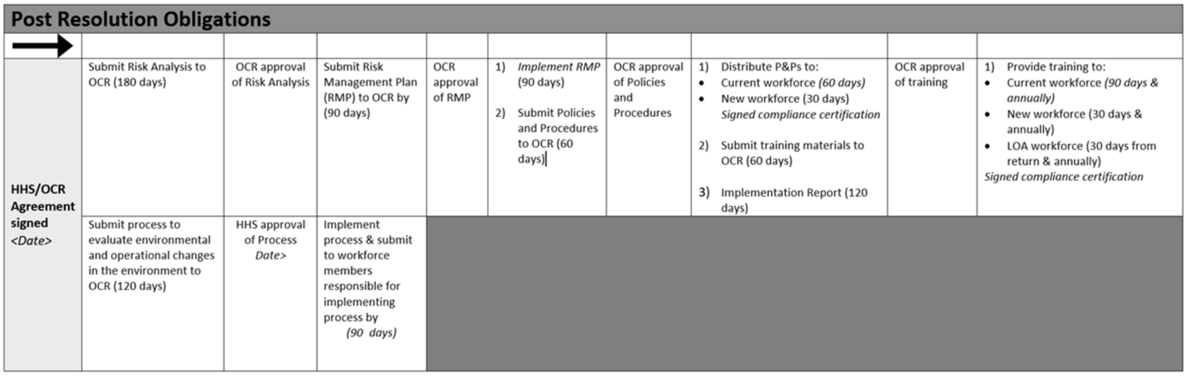
Changes:

- People (transition planning)
- Process (ensuring stakeholders & leadership are aware of ongoing CAP)

Timing:

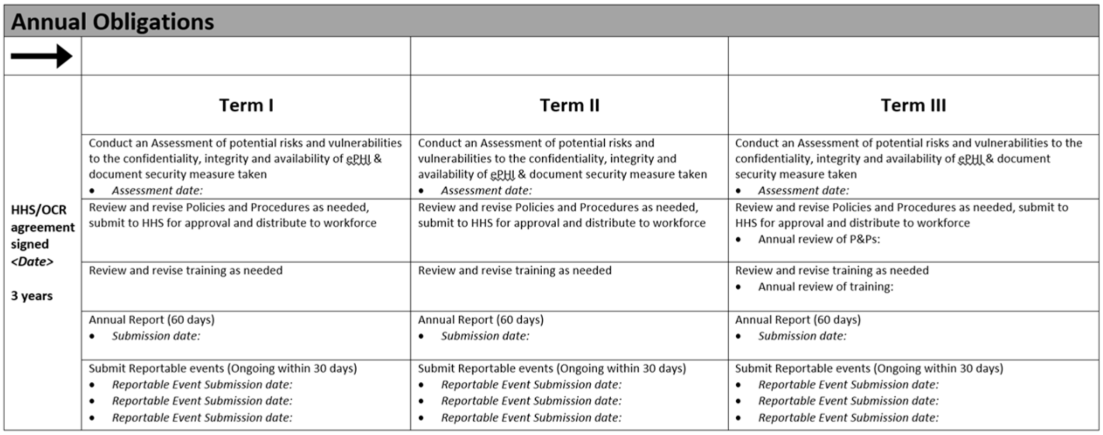
- Expectations
- The unknown

# Timelines are complicated



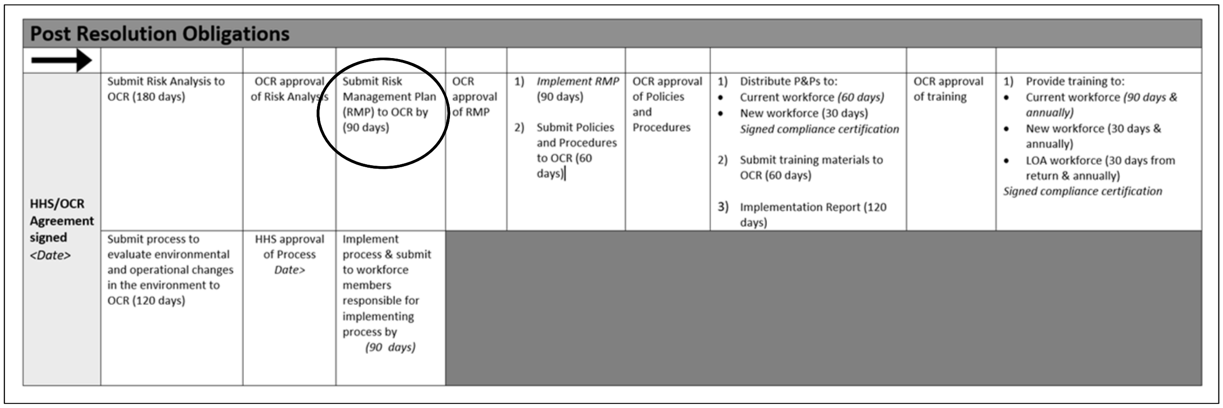
| Post Resolution Obligations | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| → | | | | | | | | | |
| **HHS/OCR Agreement signed** *<Date>* | Submit Risk Analysis to OCR (180 days) | OCR approval of Risk Analysis | Submit Risk Management Plan (RMP) to OCR by (90 days) | OCR approval of RMP | 1) *Implement RMP* (90 days)<br>2) Submit Policies and Procedures to OCR (60 days) | OCR approval of Policies and Procedures | 1) Distribute P&Ps to:<br>• Current workforce *(60 days)*<br>• New workforce (30 days)<br>*Signed compliance certification*<br>2) Submit training materials to OCR (60 days)<br>3) Implementation Report (120 days) | OCR approval of training | 1) Provide training to:<br>• Current workforce *(90 days & annually)*<br>• New workforce (30 days & annually)<br>• LOA workforce (30 days from return & annually)<br>*Signed compliance certification* |
| | Submit process to evaluate environmental and operational changes in the environment to OCR (120 days) | HHS approval of Process *Date>* | Implement process & submit to workforce members responsible for implementing process by *(90 days)* | | | | | | |

# Timelines are complicated



| Annual Obligations | | | |
|---|---|---|---|
| → | | | |
| | **Term I** | **Term II** | **Term III** |
| **HHS/OCR agreement signed** *<Date>*<br>**3 years** | Conduct an Assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI & document security measure taken<br>• *Assessment date:* | Conduct an Assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI & document security measure taken<br>• *Assessment date:* | Conduct an Assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI & document security measure taken<br>• *Assessment date:* |
| | Review and revise Policies and Procedures as needed, submit to HHS for approval and distribute to workforce | Review and revise Policies and Procedures as needed, submit to HHS for approval and distribute to workforce | Review and revise Policies and Procedures as needed, submit to HHS for approval and distribute to workforce<br>• Annual review of P&Ps: |
| | Review and revise training as needed | Review and revise training as needed | Review and revise training as needed<br>• Annual review of training: |
| | Annual Report (60 days)<br>• *Submission date:* | Annual Report (60 days)<br>• *Submission date:* | Annual Report (60 days)<br>• *Submission date:* |
| | Submit Reportable events (Ongoing within 30 days)<br>• *Reportable Event Submission date:*<br>• *Reportable Event Submission date:*<br>• *Reportable Event Submission date:* | Submit Reportable events (Ongoing within 30 days)<br>• *Reportable Event Submission date:*<br>• *Reportable Event Submission date:*<br>• *Reportable Event Submission date:* | Submit Reportable events (Ongoing within 30 days)<br>• *Reportable Event Submission date:*<br>• *Reportable Event Submission date:*<br>• *Reportable Event Submission date:* |

## Guess how far we are…



| Post Resolution Obligations | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| → | | | | | | | | | |
| **HHS/OCR Agreement signed** *<Date>* | Submit Risk Analysis to OCR (180 days) | OCR approval of Risk Analysis | Submit Risk Management Plan (RMP) to OCR by (90 days) | OCR approval of RMP | 1) *Implement RMP* (90 days)<br>2) Submit Policies and Procedures to OCR (60 days) | OCR approval of Policies and Procedures | 1) Distribute P&Ps to:<br>• Current workforce *(60 days)*<br>• New workforce (30 days)<br>*Signed compliance certification*<br>2) Submit training materials to OCR (60 days)<br>3) Implementation Report (120 days) | OCR approval of training | 1) Provide training to:<br>• Current workforce *(90 days & annually)*<br>• New workforce (30 days & annually)<br>• LOA workforce (30 days from return & annually)<br>*Signed compliance certification* |
| | Submit process to evaluate environmental and operational changes in the environment to OCR (120 days) | HHS approval of Process *Date>* | Implement process & submit to workforce members responsible for implementing process by *(90 days)* | | | | | | |

## Discover what complex organizations should consider in their training programs

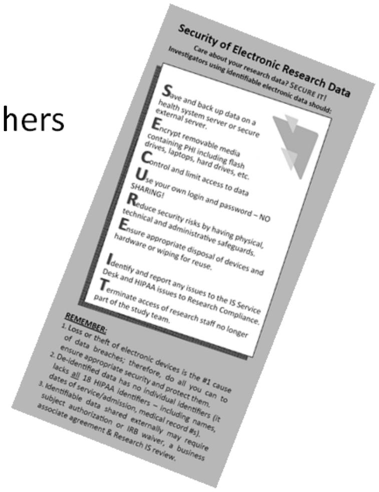
## Focus on Implementing Controls

Communication & Dissemination of Policies

Education & Training Programs for Researchers

- Research orientation/onboarding for researchers
- Ongoing HIPAA training
- Development of tools & guidance

→ *Increasing awareness is key*



**Security of Electronic Research Data**

**Care about your research data? *SECURE IT!***

**Investigators using identifiable electronic data should:**

**S**ave and back up data on a health system server or secure external server.

**E**ncrypt removable media containing PHI including flash drives, laptops, hard drives, etc.

**C**ontrol and limit access to data

**U**se your own login and password – NO SHARING!

**R**educe security risks by having physical, technical and administrative safeguards.

**E**nsure appropriate disposal of devices and hardware or wiping for reuse.

**I**dentify and report any issues to the IS Service Desk and HIPAA issues to Research Compliance.

**T**erminate access of research staff no longer part of the study team.

**REMEMBER:**

1. Loss or theft of electronic devices is the #1 cause of data breaches; therefore, do all you can to ensure appropriate security and protect them.
2. De-identified data has no individual identifiers (it lacks all 18 HIPAA identifiers – including names, dates of service/admission, medical record #s).
3. Identifiable data shared externally may require subject authorization or IRB waiver, a business associate agreement & Research IS review.

## Focus on Implementing Controls (Continued)

Institutional HIPAA Privacy & Security Review Process for Research

- Human Research Protection Program (HRPP)
- Pre-reviews/consultations by Research IT
- Use information from process to inform education and training & guidance documents

## Monitoring & Detection

Office of Research Compliance

- Routine reviews and for-cause investigations
- Monitoring PHI
- HIPAA Rounding Audits

Working collaboratively with:

- Research IT Security/Information Systems
- Corporate Compliance
  - Software detection systems
- Researchers

→ *Information used to inform education and training*

## Evaluating Risks

Larger System Level Committees:

- Research Information Security and Compliance (RISC) Committee
- Protected Health Information (PHI) Committee
- IT Risk Governance Committee

Other Sources:

- Internal & external compliance reviews
- Risk Assessments with key stakeholders
- Evaluating regulatory environment and market trends

→ *Information used to inform education and training for broader group*

Contact us:

Emmelyn Kim
Email: ekim@northwell.edu
ekim@northwell.edu
Kathleen McGill
Email: kmcgill@northwell.edu