

**Compliance in 2025 – Hot Topics
and Stump the Chumps
April 29, 2025**

Robert Hussar, Margaret
Surowka, and Melissa Zambri



Disclaimer

This PowerPoint and the presentation of Barclay Damon LLP are for informational and educational use only. Neither the PowerPoint nor Barclay Damon's presentation should be considered legal advice. Legal advice is based on the specific facts of a client's situation and must be obtained by individual consultation with a lawyer. Should you wish to obtain legal advice regarding a specific situation, the attorneys at Barclay Damon would be happy to assist you.



HIPAA Security Rule to Strengthen the Cybersecurity of Electronic PHI

» What are you hearing about the
HHS Office for Civil Rights (OCR)
proposed changes to the HIPAA
Security Rule?



HIPAA Update: Proposed Security Rule Updates

- 1. Released:** December 27, 2024.
- 2. Comment Deadline:** March 7, 2025.
- 3. Effective Date of Final Rule:** Sixty (60) days after Final Rule's publication in the Federal Register.
- 4. Compliance Deadline:** One hundred eighty (180) days from the Effective Date for most provisions.
- 5. Business Associate Agreement Transition Period:** Additional time will be allowed to revise business associate agreements to meet updated requirements.



HIPAA Update: Proposed Security Rule Updates

- Remove the distinction between “required” and “addressable” implementation specifications and make all implementation specifications required with specific, limited exceptions.
- Require written documentation of all Security Rule policies, procedures, plans, and analyses.
- Update definitions and revise implementation specifications to reflect changes in technology and terminology.
- Add specific compliance time periods for many existing requirements.



HIPAA Update: Proposed Security Rule Updates

- Require the development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI throughout the . . . entity's electronic information system(s) on an ongoing basis, but at least once every 12 months and in response to a change in the regulated entity's environment or operations
- Require greater specificity for conducting a risk analysis. New express requirements would include a written assessment that contains, among other things:
 - A review of the technology asset inventory and network map.
 - Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI.



HIPAA Update: Proposed Security Rule Updates

- Identification of potential vulnerabilities and predisposing conditions
- An assessment of the risk level for each identified threat and vulnerability.
- Require notification of certain regulated entities within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated.
- Strengthen requirements for planning for contingencies and responding to security incidents. Specifically, regulated entities would be required to:
 - Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.



HIPAA Update: Proposed Security Rule Updates

- Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.
- Establish written security incident response plans and procedures documenting how workforce members are to report and how you will respond to suspected or known security incidents.
- Implement written procedures for testing and revising written security incident response plans.
- Require regulated entities to conduct a compliance audit at least once every 12 months.



HIPAA Update: Proposed Security Rule Updates

- Require that business associates verify at least once every 12 months for covered entities (and that business associate contractors verify at least once every 12 months for business associates) that they have deployed technical safeguards required by the Security Rule to protect ePHI through a written analysis of the business associate's relevant systems by a subject matter expert and a written certification that the analysis has been performed and is accurate.
- Require encryption of ePHI at rest and in transit, with limited exceptions.
- Require regulated entities to establish and deploy technical controls for configuring relevant electronic information systems, including workstations, in a consistent manner, including:
 - Deploying anti-malware protection.
 - Removing extraneous software from relevant electronic information systems.



HIPAA Update: Proposed Security Rule Updates

- Disabling network ports in accordance with the regulated entity's risk analysis.
- Require the use of multi-factor authentication, with limited exceptions.
- Require vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Require network segmentation.
- Require separate technical controls for backup and recovery of ePHI and relevant electronic information systems.
- Require regulated entities to review and test the effectiveness of certain security measures at least once every 12 months.
- Require business associates to notify covered entities (and subcontractors to notify business associates) upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.



An employee has appeared on one of the Medicaid Exclusion Lists.

- What do we do now?
- Can they continue to work?
- Is this a self-disclosure?

OMIG Exclusion

- » The NYS Medicaid Exclusion List identifies individuals or entities who have been excluded from participating in the NYS Medicaid program under the provisions of 18 NYCRR § 515.3 and/or 18 NYCRR § 515.7.
- » https://apps.omig.ny.gov/exclusions/ex_search.aspx (CHECK UPON HIRE AND EVERY 30 DAYS)

Effect of Exclusion

- » An excluded individual or entity **cannot be involved in any activity relating to furnishing medical care, services or supplies to recipients of medical assistance for which claims are submitted to the program,** or relating to claiming or receiving payment for medical care, services or supplies during the period of exclusion. See 18 NYCRR § 515.5 for more information regarding the effect of exclusion.

OIG Exclusion

- » OIG maintains a list of all currently excluded individuals and entities called the List of Excluded Individuals/Entities (LEIE). Anyone who hires an individual or entity on the LEIE may be subject to civil monetary penalties (CMP). To avoid CMP liability, health care entities should routinely check the list to ensure that new hires and current employees are not on it.
- » https://oig.hhs.gov/exclusions/exclusions_list.asp

Licensed Professionals

- » You should also check license status of any licensed professional who is billing under their license.
- » <https://eservices.nysed.gov/professions/verification-search>

Self-Disclosure

» You may be able to payback compensation paid as opposed claims

» [Mixed Payer Calculation Form](#)



Medicaid Exclusion Lists

- Do we need to check the Medicaid Exclusion Lists for the presence of our Board members?



Medicaid Exclusion Lists

- CMS - BEST PRACTICES FOR MEDICAID PROGRAM INTEGRITY UNITS' COLLECTION OF DISCLOSURES IN PROVIDER ENROLLMENT: State Medicaid agencies should check either the MED or the LEIE upon enrolling a provider and each month thereafter to check for exclusions. We recommend that State Medicaid agencies check the MED or the LEIE for the names of provider applicants, owners, **directors**, managing employees, and agents. We also recommend that State Medicaid agencies routinely check the EPLS for the names of provider applicants, owners, **directors**, managing employees, and agents.



Guidance to States Regarding Medicaid Exclusion Lists

- . . . will conduct exclusion checks to verify that all employees, including the President and Chief Executive Officer, members of Executive Management and the Board of Directors, and interns, have not been excluded from federal healthcare programs.



Medicaid Service Documentation

- We discovered that we are missing several Medicaid services documentation records; determined this was due to employees acting inconsistent with our record retention policy and procedure.
 - What do we do? **Hmmm ...**
 - Is this a self-disclosure? **It Depends ...**
 - If so, to what entity and what should we expect?
It Depends ...



OMIG Reform

- » Will we ever see Legislative Reform of the OMIG?

It Depends

OMIG Possible Reform (IB'sHO)

- » Delayed Recoveries
- » Corrected Claims
- » Compliance Program Implementation
- » Extrapolation
- » Defending Mid-point if request a Hearing
- » Report on impact of actions against providers


Best Strategies to Obtain OMIG Reform





Best Strategies to Obtain OMIG Reform

- » Numbers
- » Targeted hits
- » Honey / Vinegar
- » Change rules of engagement
- » Establish a rapport




When should I make a referral to the
Medicaid Fraud Control Unit vs. the Office
of the Medicaid Inspector General?

It Depends


Disclosure Factors

- » Potential for a Whistleblower
- » Conduct by Agency
- » Risk tolerance (and desire for a FCA release)
- » Advice of an **experienced** Attorney



We discovered that a Staff Action Plan was distributed to the Care Manager 30 days beyond the 60 days that is allowed under the OPWDD ADM.

- » Do we have to return every claimed billed where the distribution was late?
- » If not, what approaches should we take in evaluating this situation?
 - Day 61 until when distributed
 - Did you need the SAP?




An employee is the subject of an allegation for obstruction and our agency would like to support them through paying for their legal counsel:

- Can our agency do this? **YES**
- Can the attorney represent the employee and the agency? **Possibly**
- What is the Justice Center's position on this? **It depends**

Supporting Staff in JC matters

- » Have a policy
- » Follow your policy
- » Evaluate the facts
- » Include opportunities to change course



We use GPS in our vehicles, and we identified cases where employees have been exceeding the posted speed limit:

- Are these reportable incidents to the Justice Center?

It Depends




Driving Example

- » You are riding in the agency van with people receiving services and another staff member, who is driving the van. The driver was eating a large breakfast sandwich while driving. In order to eat the sandwich, the driver used both his hands and steered with his knees. He was driving **10 miles** over the speed limit in a well-populated area with lots of vehicular and pedestrian traffic. He **stopped abruptly frequently**. After returning to the house, some of the people riding in the van told you they were afraid they were going to get into an accident.
- » **An Overview of Reporting Requirements for Custodians**
- » **January 2019**

Is this reportable to the Justice Center?

- » **YES.** Even though there was **no accident** and people receiving services **didn't suffer a physical injury**, there was **potential for harm** because of the way the van was being driven.
- » When deciding whether there is a reasonable cause to suspect that a reportable incident occurred, you should consider your own observations, training, experience and common sense in assessing the situation. **Driving with your knees** and **speeding** in **well-populated areas** puts people receiving services at risk of being in a car accident. In this case, some of the people riding in the van **said they were afraid** they while they were riding in the van.



We use GPS in our vehicles, and we identified cases where employees have been exceeding the posted speed limit:

- How should we approach the use of GPS in Vehicles?

➤ **Very Carefully**



Artificial Intelligence (“AI”)

- AI Policies and Procedures
thoughts/recommendations?

AI and Liability

- » Anyone can be sued for almost anything.
- » The liability implications of using generative AI in healthcare exist in largely uncharted territory, as these cases have yet to be directly litigated in court.
- » Providers who accept a personalized AI recommendation to provide nonstandard care would increase their risk of medical malpractice liability.
- » What we do know - At the end of the day, it has almost always been the case that the physician is on the hook when things go wrong in patient care. Physicians can use AI to inform a decision with other information - cannot be robotic, cannot decide solely based on AI output, need to be able to show why they did what they did absent the AI.

AI and Liability

» Minimize risk:

- 1. Understand the limits of AI tools:** AI should not be seen as a replacement for human judgment. Instead, it should be used as a supportive tool to enhance clinical decisions.
- 2. Apply risk assessment tools:** It considers factors like the likelihood of errors, the potential severity of harm caused and whether human oversight can effectively mitigate these risks.

Switching EHRs

» Please review:

<https://www.healthit.gov/sites/default/files/playbook/pdf/ehr-contract-guide-chapter-9.pdf>

- › Importance of compliance and build
- › Customization
- › Length of support
- › Commitment to transition and data portability
- › Data transfer or access



Immigration Enforcement

Any thoughts on immigration enforcement issues?

- Make sure your own employee documentation is in order
- Understand what ICE can do

Unannounced ICE Visits

- » The primary agency responsible for immigration enforcement is ICE, a division of the U.S. Department of Homeland Security (“DHS”).
- » Historically, Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) did not conduct enforcement efforts in “sensitive areas” (e.g. schools, **medical or mental healthcare facilities**, places of worship, sites of funerals, weddings, or other public religious ceremonies, social service establishments, places where children gather, place where disaster or emergency relief is provided, sites of ongoing public marches, rallies, or parades). *Dept. of Homeland Security, Guidelines for Enforcement Action in or Near Protected Areas (Oct. 27, 2021).*
- » That policy was rescinded in January 2025.



Best Practices (cont'd)

- » Have policies in place
- » Designate and understand what areas are “public” versus “private” areas
 - › Public examples: lobbies, entrances, parking lots, cafeterias, hallways, and public restrooms
 - › Private examples: any area that requires a swipe to enter, areas where visitors must be announced before entry, administrative offices, kitchens, examination rooms, other areas not accessible to the public



Best Practices (cont'd)

- » Train your employees
 - › Know who to contact in the event of an unexpected visit
 - › Know the differences between administrative and judicial warrants
 - › Educate them on their rights (not required to speak to agents, may ask for supervisor)
- » Share Know Your Rights guidance or other resources with your patient population and families

Resources

- » The NYS AG's Office and Officer of the Governor published helpful guidance that link to other helpful resources and include sample warrants. There are also various Know Your Rights guides.

<https://ag.ny.gov/resources/individuals/immigrants-rights/private-non-profit-organization-guidance>

<https://ag.ny.gov/sites/default/files/2025-01/immigrationguidance-appendix-a-sample-forms.pdf>

<https://www.uscourts.gov/sites/default/files/ao093.pdf>

<https://www.nyc.gov/site/immigrants/legal-resources/know-your-rights-federal-immigration-enforcement-ice.page>

<https://www.ilrc.org/red-cards-tarjetas-rojas>

Questions





Melissa Zambri

Health Care & Human Services Practice Area Co-Chair and Health Care Team Co-Leader
mzambri@barclaydamon.com | 518.429.4229



Margaret Surowka

Health Care & Human Services Practice Area Co-Chair and Health Care Team Co-Leader
msurowka@barclaydamon.com | 518.429.4295



Robert Hussar

Of Counsel

rhussar@barclaydamon.com | 518.429.4278