



BARCLAY DAMON LLP

**ARC NEW YORK/CP STATE
COMPLIANCE & QUALITY
CONNECTIONS CONFERENCE 2023**

Melissa M. Zambri

Hot Topics in Compliance

May 2, 2023




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.



Goals

- » Popular Questions
- » Regulator Focuses
- » New Things That Are Confusing
- » Questions I Answer Where the Answer is Shocking
- » Best Practices for You
- » Make You Feel Better



Questions Where the Answer is Shocking: Access to Other Provider Records by Individuals

- » Does an individual have a right to access all of the information a covered entity maintains in the individual's medical record?
- » Yes. Except in very limited circumstances, an individual has a right to access all PHI about the individual that a covered entity (or its business associate) maintains in one or more designated record sets. A designated record set is defined to include the medical record about the individual. Thus, an individual generally has a right to access all of the information about the individual that a covered entity maintains in the individual's medical record, including information the individual provided to the covered entity herself, as well as PHI about the individual contributed to the record by other health care providers or covered entities. See 45 CFR 164.524(a)(2) – (a)(3) for the limited grounds upon which a covered entity may deny an individual access to PHI in a designated record set.

»» Maintaining Records

- » How long should we maintain records:
 - › If required for billing, 10 years.
 - › Minors is longer – 3 years after the age of majority or 10 years whichever is longer.
- » Why?
 - › Statute of Limitations on the False Claims Act is 10 years.
 - › Minor's right to sue beyond 18.
- » Other records have different retention requirements.
- » And many records do not require the originals but if you might need the record to defend a fraud claim, you might need the original.



COVID-19 Public Health Emergency Unwinding Guidance

- **PowerPoint from OPWDD's PHE Unwinding Presentation to Provider Associations.** An overview of the unwinding guidance.
- **End of PHE Unwinding Guidance Memo.** This memo details flexibilities that are ending contained in the Appendix K Waiver, Medicaid Disaster Relief State Plan Amendment, and 1135 Authority.
- **PHE Flexibilities Unwinding Table.** OPWDD developed a quick reference table that details each PHE flexibility and when the provisions of the flexibility sunsets. While most will conclude on 11/11/2023, others are concluding on 5/11/2023, remain under review, or will continue after the PHE ends. As there are several flexibilities that pertain to Care Planning and Staff Action Plan activities, review this chart closely to determine what service plans need to be identified for update.



COVID-19 Public Health Emergency Unwinding Guidance

- **Care Coordination Organization Provider Policy Guidance and Manual Updates.** This memo addresses flexibility that was afforded to CCOs during the PHE. Review Staff Action Plan and life Plan requirements.
- **Care Management Report Technology (Telehealth) Service Delivery Policy.** This policy details the allowance of the use of remote technology to meet the face-to-face contract requirements of Care Management. Please note that the annual Life Plan meeting must still occur in-person. A person may choose to participate in meetings using remote technology at other times during the year.



Life Plan Finalization

- » Service providers are responsible for reviewing the finalized, acknowledged and agreed to Life Plan.
- » If there are inaccuracies, providers should demonstrate due diligence in working with the Care Manager, CCOs, OPWDD and/or others to correct the Life Plan as soon as possible.
- » Service providers should document their timely efforts to correct any errors in the Life Plan. Examples of this documentation may include notes in the individual's monthly summary, e-mails, phone calls, etc.
- » You are trying to show that it is not your fault.

Waiver Service Provision

- » If a new Life Plan is not finalized in the expected timeframe, the services do not expire (i.e., the service remains authorized by the DDRO for the individual) but we want to do everything we can to avoid billing disallowances in a fiscal audit.
- » For these reasons, make sure your process is followed – do what you need to do on a timely basis and point out any mistakes made by the Care Manager.



Sharing Salary Data

- » The Department of Justice withdrew three policy statements on health care antitrust enforcement, saying they are “overly permissive on certain subjects, such as information sharing,” and that “a case-by-case enforcement approach” would allow it to better evaluate health care mergers and competition.
- » Information exchanges, in and of themselves, are not per se illegal under the Sherman Act. Courts have acknowledged that there can be legitimate, procompetitive reasons for exchanging information, and thus such exchanges are judged under the Rule of Reason, which is a balancing test that takes into account all of the facts and circumstances and then determines whether the anticompetitive effects outweigh the procompetitive benefits of the restraint.

»» Sharing Salary Data

- » That said, courts have prohibited information exchanges in industries with structural characteristics (e.g., high concentration), where such exchanges may be more likely to have anticompetitive effects. See *U.S. v. Container Corp.*, 393 U.S. 333 (1969) (prohibiting price verification practices in a concentrated industry). Additionally, although not itself illegal per se, proof that competitors have shared price information sometimes has served as evidence of a per se illegal conspiracy. Accordingly, exchanging competitively sensitive information, particularly with competitors, has always been a practice that requires careful review and safeguards. Those safeguards have historically been structured based on guidance from U.S. antitrust enforcement agencies.
- » For more information regarding practical guidance, see nurse wage lawsuits.

This Guidance Was Revoked

- » The 1996 Guidance stated that industry surveys concerning prices, wages, salaries, or benefits were unlikely to violate the antitrust laws and would not be prosecuted by the agencies, absent extraordinary circumstances, if they satisfied three conditions:
 - › The survey was managed by a third party (e.g., a purchaser, government agency, health care consultant, academic institution, or trade association);
 - › The information shared was more than three months old; and
 - › The information was sufficiently aggregated such that no recipient could identify the prices charged or compensation paid by any particular provider (e.g., there were at least five participants reporting data and no individual participant's data represented more than 25% on a weighted basis of that statistic).

- » Without this in place any longer, sharing this information is more risky even if done in this way.

Sharing Salary Data

- » In announcing the withdrawal of the policy, Principal DAAG Mekki stated, “exchanges facilitated by intermediaries can have the same anticompetitive effect as direct exchanges among competitors. In some instances, data intermediaries can enhance—rather than reduce—anticompetitive effects.”
- » The Division no longer believes an exchange of historic data necessarily reduces the risk of anticompetitive harm due to advances in artificial intelligence. Principal DAAG Mekki stated, “the suggestion that data that is at least three-months old is unlikely to be competitively-sensitive or valuable is undermined by the rise of data aggregation, machine learning, and pricing algorithms that can increase the competitive value of historical data for some products or services.”

The New Compliance Regulations

- » Confusion:
 - > Work Plans
 - > Contractors
 - > Training
 - > Changes

Compliance Work Plans

- » Aspirational and realistic
- » Flexible
- » Get buy-in
- » Build in room for the unexpected



Reinvigorating Your Compliance Plan (Cont.)

- » Has anyone surveyed staff (e.g., what is working, what is not working, what they know)?
- » Has anyone interviewed staff regarding the plan (e.g., where they think weaknesses are, best practices from other employers, how you are doing)?



Compliance Work Plans: Risk Assessments

- » Get together the group of people that makes sense (e.g., compliance committee, program and department managers, etc.).
- » What has changed?
- » What is changing?



Compliance Work Plans: Risk Assessments (Cont.)

- » Audit protocols
- » Government work plans
- » Enforcement experience (e.g., your agency and your colleagues at other agencies)
- » Known problems
- » Complaints or grievances



Compliance Work Plans: Risk Assessments (Cont.)

- » Process changes
- » Personnel changes
- » Management changes
- » Vendor changes

Compliance Work Plans

- » Assess the risks
- » Prioritize
- » Use of resources
- » Creation of work plan

Items to Remember

- » Identifying and prioritizing risks is not an action plan.
- » Audits are not corrective action.
- » Understand the root cause.

Audit Protocols

- » “Audit protocols assist the Medicaid provider community in developing programs to evaluate compliance with Medicaid requirements under federal and state statutory and regulatory law. Audit protocols are intended solely as guidance in this effort. This guidance does not constitute rulemaking by the New York State Office of the Medicaid Inspector General (OMIG) and may not be relied on to create a substantive or procedural right or benefit enforceable, at law or in equity, by any person.”

Audit Protocols (Cont.)

- » “Furthermore, nothing in the audit protocols alters any statutory or regulatory requirement and the absence of any statutory or regulatory requirement from a protocol does not preclude OMIG from enforcing the requirement. In the event of a conflict between statements in the protocols and either statutory or regulatory requirements, the requirements of the statutes and regulations govern.”

Audit Protocols (Cont.)

- » “A Medicaid provider’s legal obligations are determined by the applicable federal and state statutory and regulatory law. Audit protocols do not encompass all the current requirements for payment of Medicaid claims for a particular category of service or provider type and, therefore, are not a substitute for a review of the statutory and regulatory law. OMIG cannot provide individual advice or counseling, whether medical, legal, or otherwise.”

Audit Protocols (Cont.)

- » “In this effort, OMIG will review and consider any relevant contemporaneous documentation maintained and available in the provider’s records to substantiate a claim. OMIG, consistent with state and federal law, can pursue civil and administrative enforcement actions against any individual or entity that engages in fraud, abuse, or illegal or improper acts or unacceptable practices perpetrated within the medical assistance program.”

Internal Investigations



»» Questions to Consider

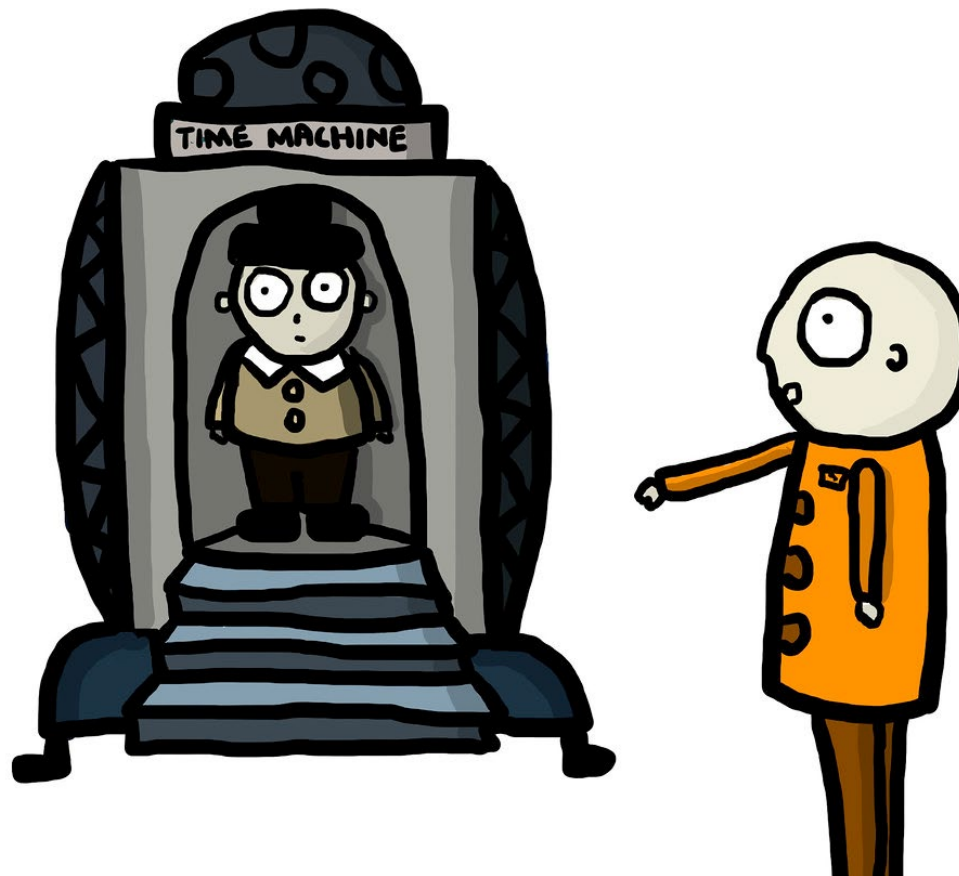
- » What do you need to investigate?
- » Who should conduct the investigation (e.g., compliance, HR, counsel)?
- » How should you document?
- » Who do you report to?



Gathering the Evidence

- » Keep notes
- » Summarize what has been done
- » Enlist help of program staff/billing
- » Reach out to counsel with questions
- » Keep Attorney-Client Communication Privileged & Confidential

Going Back in Time



How Far Back Should You Go?

- » Start small.
- » Go further if necessary.
- » Get counsel involved if necessary.

»» Make a Plan for Investigation

» Scope?

- › Possible causes
 - Clinician start date
 - Rule changes
 - Management or personnel changes
 - Change in policies
 - IT issue
 - Other issues

Reports

- » Be careful of your language (e.g., fraud, breach)
- » Privileged and confidential
- » Counsel involvement
- » Mindful of discovery

Self-Disclosure

- » The language giving discretion appears gone.
- » What do we do now?
 - › OMIG has been quoted as saying that they know there needs to be guidelines but they would not commit to them yet

Contemporaneous

- » To prepare and to maintain contemporaneous records demonstrating its right to receive payment under the medical assistance program and to keep for a period of six years from the date the care, services or supplies were furnished, all records necessary to disclose the nature and extent of services furnished and all information regarding claims for payment submitted by, or on behalf of, the provider and to furnish such records and information, upon request, to the department, the Secretary of the United States Department of Health and Human Services, the Deputy Attorney General for Medicaid Fraud Control and the New York State Department of Health.
- » How can it be defined? Current audits.



The New Compliance Regulations: Framework

- » Purpose: Detect and prevent fraud, waste, and abuse in the Medicaid Program.
 - › Organize provider resources to address compliance issues as quickly and efficiently as possible.
 - › Impose systemic checks and balances to prevent future recurrence of such issues.

- » Requirement: Providers must adopt, implement, and maintain an effective Compliance Program.
 - › Must be tailored to fit its specific organizational needs.
 - › Size, complexity, resources, and culture.

»» Affected Individuals

- » “[A]ll persons **who are affected by the required provider’s risk areas** including the required provider’s employees, the chief executive and other senior administrators, managers, contractors, agents, subcontractors, independent contractors, and governing body and corporate officers.”

Risk Areas

1. Billings.
 2. Payments.
 3. Ordered services.
 4. Medical necessity.
 5. Quality of care.
 6. Governance.
 7. Mandatory reporting.
 8. Credentialing.
 9. Contractor, subcontractor, agent, or independent contractor oversight.
 10. Other risk areas that are or should reasonably be identified by the provider through "organizational experience."
- » Note: There are additional risk areas for MMCOs.



Risk Areas: Organizational Experience

- » Knowledge, skill, practice and understanding in operating your Compliance Program.
- » Identification of any issues or risk areas in the course of your internal monitoring and auditing activities.
- » Experience, knowledge, skill, practice, and understanding of your participation in the Medicaid Program and the results of any audits, investigations, or reviews you have been the subject of.
- » Awareness of any issues you should have reasonably become aware of for your categories of service.

Effective Compliance Program

» OMIG Guidance

- › Should be reasonably designed, implemented, and enforced so that the program is generally effective in preventing, detecting, and correcting fraud, waste, and abuse, and non-compliance with Medicaid Program requirements.
- › “The failure to prevent or detect an individual or unique compliance issue does not necessarily mean that the program is not generally effective.”



Contractors

- » Contractors, agents, subcontractors, and independent contractors are affected individuals if they are affected by compliance risk areas.
- » Contractor oversight expressly included as a risk area.
- » Contractual Requirements: Contracts must:
 - › Specify that the contractor is subject to the provider's Compliance Program requirements.
 - › Include termination provisions for failure to adhere to Compliance Program requirements.

Contractors (cont.)

» OMIG Guidance

- › Only subject to the Compliance Program to the extent it is related to contracted role and responsibilities within the identified risk area.
 - Example: Contractors who provide credentialing services would be required to comply with policies and procedures, training, etc., as it relates to the provision of credentialing services.
- › Contracts that are new or renewed after March 28 must include the new contract provisions.
- › Contractors who are required providers should work with providers it contracts with to determine how to implement the regulatory requirements in the most efficient manner possible.

»» Time Periods

- » Amended regulations lay out specific time frames in various areas.
- » For example:
 - › Policies, Procedures, and Standards of Conduct = Annual review.
 - › Training and Education = Orientation, “promptly” upon hiring, and (at least) annually.
 - › Compliance Program Review = Annually.
 - › Exclusion Checks = Every 30 days.



Written Policies & Procedures (cont.)

» Disseminating Information

- › Providers must post information on the Compliance Program, including the Standards of Conduct, on their website.
- › Written policies and procedures must be available, accessible, and applicable to all affected individuals.

»» Compliance Officer (cont.)

- » New responsibilities examples:
 - › Draft, implement, and update a compliance work plan for the coming year, no less than annually or as otherwise necessary.
 - › Report no less than quarterly to the governing body, chief executive, and Compliance Committee on the progress of adopting, implementing, and maintaining the Program.
 - › Coordinate with a designated Compliance Committee.
 - › Investigate and independently act on matters related to the Compliance Program.

»» Compliance Officer (cont.)

»» **OMIG Guidance**

- › Expectation that the Compliance Officer coordinates the implementation of the work plan.
- › Compliance Officer reporting to general counsel or financial officer creates risk to establishing an effective Compliance Program.
 - If not feasible, should create a procedure for addressing conflicts of interest or potential risks.
- › OMIG will consider provider's documented good faith efforts to hire and retain staff.

Compliance Committee

- » Must have a charter, which must be reviewed and updated at least annually.
 1. Duties.
 2. Responsibilities.
 3. Membership (at a minimum, senior managers).
 4. Designation of Chair (Compliance Officer).
 5. Frequency of Meetings (no less than quarterly).
- » Report directly and accountable to CEO and Board.
- » Operations, finance, audit, HR, utilization review, social work, discharge planning, medicine, coding, legal, key operating units.

»» Compliance Committee (cont.)

- » Committee will also be responsible for:
 - › Advocating for the allocation of sufficient funding, resources, and staff to allow the Compliance Officer to fully perform their responsibilities.
 - › Collaborating with the Compliance Officer on written policies and procedures.
 - › Advocating for the enactment of required modifications to the Compliance Program.



Compliance Training & Education (cont.)

At a minimum, must include discussion of:

1. Risk areas and organizational experience.
2. Role of the Compliance Officer and Compliance Committee.
3. Obligation to report compliance concerns, reporting procedures, and non-intimidation and non-retaliation policies.
4. Disciplinary standards.
5. Corrective action plans and response to compliance issues.
6. Medicaid Program requirements and the provider's category of services
7. Coding and billing requirements and best practices.
8. Claim development and submission.



Compliance Training & Education (cont.)

- » Must develop and maintain a **training plan** that outlines:
 1. Subjects or topics for training and education.
 2. Timing and frequency of the training.
 3. Which affected individuals are required to attend.
 4. How attendance will be tracked.
 5. How the effectiveness of the training will be periodically evaluated.
- » Impact = Off-the-shelf, generic compliance training modules will likely need to be supplemented to comply with the new requirements.



Compliance Training & Education (cont.)

» **OMIG Guidance**

- › Training may be customized, so long as everyone receives training in the core compliance topics.
- › Distribution only is not effective training and education.
- › Self-study programs may be acceptable when the provider can produce evidence that individuals have received and appropriately applied the subject matter.
- › Dated distribution letter or acknowledgement for contractors.



Compliance Training & Education (cont.)

» **OMIG Guidance – Training Plans**

- › List of all affected individuals that received, and did not receive Compliance Program training during the review period (name and type).
- › Type of compliance training(s) received (annual, orientation, or both).
- › How training was provided.
- › Dates of completion.
- › Dates of hire for those who received orientation training.



Boards – Annual Training Content

- » Updating training:
 - › Duties
 - › Conflict of Interest
 - › Roles and Responsibilities
 - › Compliance
 - › Quality
 - › HIPAA

»» Lines of Communication

- » Must establish and implement effective lines of communication which ensure confidentiality for affected individuals.
- » Need anonymous method to report.
- » Provider must “ensure that the confidentiality of persons reporting compliance issues shall be maintained unless the matter is subject to a disciplinary proceeding, referred to, or under investigation by, MFCU, OMIG or law enforcement, or disclosure is required during a legal proceeding, and such persons shall be protected under the required provider’s policy for non-intimidation and non-retaliation.”

»» Auditing & Monitoring

» Audit Program

- › Must be formalized and focused on risk areas.
- › Performed by internal/external auditors who:
 - Have expertise in state and federal Medicaid Program requirements and applicable laws, rules, and regulations; or
 - Have expertise in the subject area of the audit.

»» Auditing & Monitoring (cont.)

» Audit Program (cont.)

- › Document the design, implementation, and results of internal and external audits.
- › Share the results with the Compliance Committee and governing body.
- › Review audit results for risk areas that can be included in updates to Compliance Program and work plan.
- › Report, return, and explain overpayments identified.

Auditing & Monitoring (cont.)

» **Annual Effectiveness Review**

- › Must be performed annually to determine whether Compliance Program requirements in Part 521-1 are being met.
 - Is the compliance program effective?
 - Are any revisions or corrective actions needed?
- › This is in addition to auditing to monitor compliance with Medicaid billing requirements.
- › Compliance Officer, Compliance Committee, external auditors, or other staff (knowledge, experience, and independence).

»» Auditing & Monitoring (cont.)

» Annual Effectiveness Review (cont.)

- › Annual Effectiveness Review should include:
 1. On-site visits.
 2. Interviews with affected individuals.
 3. A review of records, surveys, and other methods.
- › Process for and the results of the review must be documented and shared with the CEO, senior management, Compliance Committee, and Board.

»» Responding to Compliance Issues

- » Investigations must be documented.
 1. Any alleged violations.
 2. A description of the investigative process.
 3. Copies of interview notes.
 4. Other documents essential for demonstrating that the provider completed a thorough investigation of the issue.
- » Must promptly report credible evidence that a state or federal law, rule, or regulation has been violated to the appropriate governmental entity.
 - › Compliance Officer must retain reports made.



OMIG Compliance Program Reviews

» OMIG Guidance

- › Will evaluate performance for each requirement and assess a score per month of each question.
- › Average score will be used to determine whether the requirements have been met for the review period.
 - > 60% is satisfactory.
 - < 60% is unsatisfactory and may result in a monetary penalty.
- › Each provider's unique characteristics will be taken into consideration.



Other Hot Topics





Personal Devices

- » Must maintain confidentiality and protect from unauthorized disclosure, loss or use of such information
- » If not, discipline
- » No access for those who do not need it for job functions
- » No sharing access
- » Limit storage of EPHI on device
- » Only store information as allowed
- » No pictures unless required for your job
- » Strong security
- » If stolen, advise IT Department
- » Agree to remote wipe
- » Monitored if connected to network
- » Reserves right to inspect, seize and hold



Breach Notification Requirements



SHIELD Act Notifications

- » **For breaches of “Private Information,” entities must notify:**
 - › NYS Attorney General
 - › NYS Department of State
 - › NYS Division of State Police regarding the timing, content, and distribution of the notices and the approximate number of affected individuals
- » **For breaches of PHI (even if not “private information”):** Covered Entity must notify the NYS Attorney General **within 5 business days of notifying the HHS-OCR**

Texting

- » Requirements of Security on Equipment
- » Verifying number
- » Maintaining information on phone
- » Limiting content
- » Encouraging call

Texting

- » Tone
- » Cost to individual
- » Expectations regarding response
- » Individuals in crisis

Ransomware in the News



**Don't
click on
the link!**



**HHS Update #3: International Cyber Threat
to Healthcare Organizations (Resend)**

May 15, 2017

Ransomware

- » Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., “watch this video, it’s amazing”);
- » Be suspicious of clickbait titles (e.g., offering prizes, advice);
- » Check email and names of people they received a message from to ensure they are legitimate;
- » Look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks);
- » If an employee is unsure that an email is safe they should refer said email to the IT Department.

Keeping Information Secure

- » Turn off screens and lock devices when leaving desk;
- » Report stolen or damaged equipment as soon as possible;
- » Change all account passwords immediately when a device is stolen;
- » Report a perceived threat or possible security weakness in agency systems;
- » Refrain from downloading suspicious, unauthorized or illegal software on their company equipment;
- » Avoid accessing suspicious websites.



Office of Civil Rights (OCR) HIPAA Right of Access Initiative





HIPAA Right of Access: New York Preemption

- » HIPAA: generally require covered entity health care providers to provide medical records within 30 days of the request and only charge a reasonable cost-based fee
 - » New York: Under New York Public Health Law §18, a health care provider has only 10 days to respond to a written request for providing patient information.
- » Right of access extends to an individuals’ “personal representatives” as well
 - » In New York, those individuals are referred to as “qualified persons” listed under section 18(g) of the Public Health Law

»» HIPAA Right of Access

- » 2019: HHS OCR announces “Right of Access Initiative”
- » Promise to enforce the rights of patients to receive copies of their medical records promptly and without being overcharged and in the readily producible format of their choice
- » To date, OCR has settled 42 “right of access” investigations.

»» Corrective Action and Monitoring

- » In addition to monetary settlements, CEs were subject to detailed corrective action plans (CAPs), which include one to two years of monitoring by OCR.
- » If the agreement is breached, HHS can impose civil monetary penalties.



HIPAA Right of Access: Summary

- » Initiated by complaints
 - › Individuals
 - › Personal representatives
- » Violations include:
 - › Lack of timely access
 - › Fees not reasonable
 - › Not in requested format
- » Takeaway: Have policy/procedure in place to timely process medical record requests.

»» Popular Telephone Calls

- » Facebook Live
- » Snapchat
- » Ransomware/Hacking/Spoofs
- » Texting Wrong Person
- » Talking About Service Recipients in the Public
- » Encryption

Thank You



Melissa M. Zambri

Partner

Health Care & Human Services Co-Team Leader

Barclay Damon LLP

80 State Street

Albany, New York 12207

P: (518) 429-4229

M: (518) 369-8615

mzambri@barclaydamon.com