BARCLAY DAMON LLP

Compliance 2020-2021: It was already hard without COVID

Melissa M. Zambri, Esq.

January 21, 2021

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. Please consult a healthcare attorney before attempting to address any legal situation raised in this seminar.

Agenda

1. 2020 – It's over. Why do I feel just as stressed?
2. Hot Topics
    1. Compliance Program
    2. Audits
    3. COVID
    4. Privacy/Security Abbreviated

Compliance Program Changes

Overpayments

- A recipient of a Medicaid Program overpayment must:
  - Report and return the overpayment to the DOH; and
  - Must notify the OMIG (in writing) of the reason for the overpayment
- Overpayments must be returned within 60 days from:
  - When it was identified; or
  - The date any corresponding cost report is due
- A voluntary self-disclosure program was memorialized

New Subsections 5 and 6: Report, Return, Explain

- “Identification” of an overpayment occurs:
- When the person knows or should have known through the exercise of reasonable diligence, that they <u>received an overpayment and quantified the amount of the overpayment</u>.
- 60 day clock starts ticking when you knew or should have known you received an overpayment <u>and</u> quantified the amount.
- Quantification of the amount can be time-consuming.

Statutory Changes to Compliance Programs

- Requires a compliance committee.
- Requires annual training and required training for Board.
- New monetary penalties for not having a plan considered effective ($60,000 on first finding, doubled on second finding).
- Memorializes interest on overpayments but allows OMIG to waive. Requires repayment in 15 days of confirmation by OMIG but sets forth it can be longer if there is an approved hardship request. Memorializes OMIG's ability to require a compliance agreement and terminate participation for failure to comply.
- Waiting for regulations.

Statutory Changes to Compliance Programs

- Previously, SSL 363-d required a provider's Non-Intimidation/Non-Retaliation policy protect persons for reporting to appropriate officials "as provided in section 740 and 741 of NY Labor Law"
- The reference to the Labor Law provisions has been deleted.
- Expands the required protection to any report to government officials.

Statutory Changes to Compliance Programs

- Previously, disciplinary policies had to provide sanctions specifically for:
  - 1) failing to report suspected problems;
  - 2) participating in non-compliant behavior;
  - 3) encouraging, directing, facilitating or permitting non-compliant behavior.
- Now, amendments deleted 1, 2, and 3 but regulations require so retain.
- New requirement: Make sure disciplinary policies are "well publicized".

Statutory Changes to Compliance Programs

- » Previously required: "A system for routine identification of compliance risk areas specific to provider type, for self evaluation of such risk areas, including internal audits and as appropriate external audits, and for evaluation of potential or actual non-compliance as a result of such self evaluations and audits.

Statutory Changes to Compliance Programs

- Now required: "Establishment and implementation of an effective system for routine monitoring and identification of compliance risks. The system should include internal monitoring and audits and, as appropriate, external audits, to evaluate the organization's compliance with the medical assistance program requirements and the overall effectiveness of the compliance program."

Penalties For Failure to Meet Compliance Program Requirements

- Amendment states that compliance program requirements set forth in SSL 363-d are a condition of Medicaid payment.
- Effective 4/1/20
- OMIG can now recoup Medicaid payments from a provider during period it determined the Compliance Program did not satisfy SSL 363-d requirements.

Compliance Reviews

- Compliance Reviews begin January 2021
- Important to evaluate your Compliance Program prior to this date
- Good starting point: https://omig.ny.gov/compliance/compliance-library

Annual Certifications

- OMIG and DRA certifications are combined in one certification since DRA requirements are required under SSL 363-d
- Now included in provider's electronic Certification for Provider Billing Medicaid due on annual anniversary of enrollment

Audits

COVID-19 Funding

- Many funding streams.
- Process of meeting requirements can be similar.

Federal Paycheck Protection Program

- PPP borrowers were required to certify in good faith that:
  - Their PPP loan request was necessary;
  - Current economic uncertainty made the loan request necessary to support their ongoing operations; and
  - Funds only used to retain workers and maintain payroll or make mortgage interest payments, lease payments, and utility payments.
- All PPP loans of more than $2 million will be investigated by the federal government, and are subject to audit by the SBA and Treasury.

Federal Monies

- Providers receiving distributions must:
  - Agree to terms and conditions, including various certifications
  - Accept or return funds
  - Sign an attestation
- Maintain documentation to back request, criteria, your thought process, how the money was spent, etc.

Focus on Fraud

- Providers will likely see increased enforcement and investigation activities related to COVID-19
- Enforcement and investigation are likely to be decentralized
- Documentation will be important
- Review, audit, and enforcement should be assumed

Focus on Fraud, cont.

“Every U.S. Attorney’s Office is hereby directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic.”

– A.G. William Barr

“Attorney General William P. Barr is urging the public to report suspected fraud schemes related to COVID-19. . . . Some examples of these schemes include . . . Medical providers obtaining patient information for COVID-19 testing and then using that information to fraudulently bill for other tests and procedures.”

- DOJ Press Release

Pandemic Response Accountability Committee

- Oversight body created by the CARES Act
- Charged with preventing and detecting fraud, waste, abuse, and mismanagement of funds
- Also responsible for randomized audits

OPWDD/OMIG Audits

- They are moving again
- Exit conferences by video
- Interesting focus of desk audits on whether or not ordering providers are enrolled with Medicaid based on CMS guidance and sometimes older Medicaid updates

Agency Review

- Did you try to read the 362 pages and prepare responses?
- Do you have a binder? Do you know where it is? Is it updated?
- Who has the thickest binder?
- We expect these to move in 2021 – easy to do offsite, particularly if you have a binder.

PERM Audits

- CMS will be measuring improper payments in the Medicaid Program under the Payment Error Rate Measurement (PERM) program. Due to the pandemic, CMS in April had suspended all PERM engagement/communication or data requests to providers and state agencies. Effective 8/11/20, CMS resumed PERM-related engagements, including New York.
- Did you get a request for a claim or two?
- The number they give you should identify what type of claim you billed.
- The list of documents they want will not look relevant to your services. They want the documentation allowing you to bill but the list will look more like you are a hospital or physician's office. Give them what they want under the audit protocol.

BREATHE IN AND OUT BREAK

COVID-19 Compliance Issues

COVID WAIVERS: Compliance Issues to Consider

- New day, new billing
- Telehealth – documentation good enough?
- Services in different settings – are you clear about where services are being provided?
- Changes to services – updated in Life Plan as soon as possible, but not later than 60 days after approval of service or change.

COVID WAIVERS: Compliance Issues to Consider

- Staff Action Plans must be updated, although timelines have been waived until 60 days following the cessation of the state of emergency.
- Who is providing the services – your CFR and making sure people are assigned correctly.
- The person who provided the service should document the service.

COVID WAIVERS: Compliance Issues to Consider

- Students in the virtual world – waiver services can be provided during traditional school hours, but outside the scheduled time for instruction provided to the child.
- Day services in an ICF – 7/22/20-10/14/20, memo dated 9/18/20

COVID WAIVERS: Compliance Issues to Consider

- Respite memo
- Supported employment memo
- Day hab and site-based prevoc after the retainer program memo
- Article 16 memo

Waivers: HIPAA & Telehealth

- HHS OCR published Notice of Enforcement Discretion providing that penalties will not be imposed on providers serving patients in good faith through communication technologies during the public health emergency
- Use of popular applications allowing for video chats is permissible, but public facing communication applications are prohibited
- Permitted applications may be used to provide telehealth services outside of COVID-19 treatment and without having a valid BAA in place
- But, providers must still take steps to reasonably ensure privacy

Waivers: HIPAA & Telehealth

- The U.S. Department of Health and Human Services Office of Civil Rights (OCR) recently announced that telehealth providers must have a Business Associate Agreement in place and telehealth services must be provided on a HIPAA-compliant program by January 21, 2021.
- But then the waiver was extended to April 21, 2021 so we might as well start to prepare.

Practical Guidance: Suggestions for Effective & Legal Telepractice

- Develop procedures for and obtain informed consent before providing remote services
- Ensure that informed consent includes both benefits and risks
- Conduct an initial assessment to determine whether telepractice is appropriate
- Attend to issues of danger to self or others and to mandated reporting requirements in accordance with law
- Make arrangements, if needed, in the individual's local area to address emergency and crisis situations that may arise, and be knowledgeable of community resources

Practical Guidance: Suggestions for Effective & Legal Telepractice

- Ensure the accuracy of advertising and public statements about telephone and online services offered and do not imply a level of treatment or effectiveness that is beyond what is actually provided
- Remain aware of the limitations of the online services provided and the technology used
- Evaluate and modify online services offered to ensure their effectiveness

Practical Guidance: Suggestions for Effective & Legal Telepractice

- Employ professional standards of practice including adequate documentation and record keeping
- Attend to cultural, ethnic, language, and other differences that may impact the ability to effectively communicate with and treat individuals

Adirondack Health Institute Guidance

Key questions you will want answered when exploring telehealth platforms:

- Can I exit my contract at any time?
- Is there a waiting room feature so I can queue people up?
- Is the platform device agnostic (i.e., can providers and individuals use the device of their choosing)?
- Does the software have the ability to schedule a visit?
- How long to deploy platform?

EVV

- You know what is great in a pandemic?
  - Implementing a new program to track employees and services.

EVV

» What it is meant to do

- Verify visits in real-time, including date, location, type of service, individual(s) providing and receiving services, and duration of service(s)
- Validate hours of work for home health employees
- Eliminate billing data entry mistakes
- Reduce costs related to paper billing and payroll
- Help combat fraud, waste, and abuse

EVV

» Things to think about

- Can the person still check in and drive away – do you still spot check, do you still do receipts of visits?
- Do you have two systems of verifying time that now may conflict – like a payroll system and a system capturing time?
- How are you going to handle when someone forgets to clock in or out?
- Who got stuck being the EVV expert?

Privacy/Security Abbreviated

HIPAA and COVID-19: February Bulletin

- Describes ways PHI may be shared during emergency situation under HIPAA
- HIPAA allows disclosures of PHI without authorization to:
  - Public Health Authorities, such as CDC or state/local health department authorized by law to collect such information to prevent or control disease (includes disease reporting, public health surveillance, investigations or interventions).
  - Family, Friends, and Others Identified by Individual as Involved in the Individual's Care (should get verbal permission from individual or reasonably infer that individual does not object)

HIPAA and COVID-19: February Bulletin

- Reminds of HIPAA minimum necessary standard
  - Covered Entity must make reasonable efforts to limit information disclosed to that which is the "minimum necessary" to accomplish the purpose.
  - Example: Access to any COVID information should be very strict and limited (minimum necessary for the public health purpose).

HIPAA and COVID-19: February Bulletin

- Cautions against disclosures to the media
  - Affirmative reporting to the media or public at large about an identifiable individual generally requires written authorization.
  - Notices in interest of public health should only provide time, place and date of a possible COVID exposure.

Press Issues

OCR settled with Allergy Associates, a health care practice that specializes in treating individuals with allergies, for $125,000

- In February 2015, a patient of Allergy Associates contacted a local television station to speak about a dispute that had occurred between the patient and an Allergy Associates doctor
- OCR's investigation found that the reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed the patient's PHI to the reporter

Ransomware in the News

Don’t click on the link!

HEALTHCARE AND PUBLIC HEALTH SECTOR
Critical Infrastructure Security and Resilience Partnership
HOSPITAL

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

May 15, 2017

E-Mail Security

- Think before sending or opening.
- When opening email, ask yourself, does this email pertain to me?
  - Malicious emails
    - Malicious web links
    - Malicious attachments
    - Phishing for information
- By default, email is not a secure way to transmit information
- Never send sensitive information in an email without encryption
  - PHI
  - Social Security Numbers
  - Bank, Credit Card account information
  - Passwords

Social Media: It is Everywhere

Social Media HIPAA Violations

- Posting verbal “gossip” about an individual served to unauthorized individuals, even if the name is not disclosed
- Sharing of photographs or any form of PHI without written consent from an individual served
- A mistaken belief that posts are private or have been deleted when they are still visible to the public
- Sharing of seemingly innocent comments or pictures, such as a workplace lunch which happens to have visible individual files underneath

Yelp

OCR received a complaint from an Elite patient alleging that Elite had responded to a social media review by disclosing the patient's last name and details of the patient's health condition

- OCR determined that Elite had impermissibly disclosed the PHI of multiple patients in response to reviews on the Elite Yelp review page
- Elite did not have a policy and procedure regarding disclosures of PHI to ensure that its social media interactions protect the PHI of its patients or a Notice of Privacy Practices that complied with the HIPAA Privacy Rule
- OCR accepted a substantially reduced settlement amount in consideration of Elite's size, financial circumstances, and cooperation with OCR's investigation

"Social media is not the place for providers to discuss a patient's care," said OCR Director, Roger Severino. "Doctors and dentists must think carefully about patient privacy before responding to online reviews."

Working Remotely

- All PHI must be encrypted before being transmitted.
- Encrypt and password protect any personal devices if you use them for work.
- Do not allow any friends, family, etc. to use devices that contain PHI.
- Secure information at home.
- Shred information at home or bring it to work to shred. Do not just throw it out.
- Disconnect from the network.

Texting – Do You Have A Policy?

- 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

Questions? Comments?