COVID-19 Compliance Today and Tomorrow

Compliance Program Considerations for Provider Organizations in Response to COVID-19

Montana Hospital Association
April 30, 2020

Disclaimer

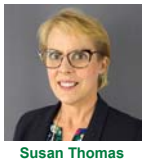
To the best of our knowledge, this information was correct at the time of publication. Given the fluid situation, and with rapidly changing new guidance issued daily, be aware that some or all of this information may have changed or no longer apply.

Please visit our COVID-19 hub frequently for the latest updates, as we are working diligently to put forth the most relevant helpful guidance as it becomes available. www.pyapc.com/covid-19-hub/

Your Presenters

Sarah Bowman
MBA, CHC®, RHIA®
Senior Manager
sbowman@pyapc.com

Barry Mathis
Principal
bmathis@pyapc.com



Susan Thomas
CHC®, CIA, CRMA, CPC®
Manager
sthomas@pyapc.com

PYA, P.C.
800.270.9629 | www.pyapc.com

ATLANTA | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

Agenda

- ✓ COVID-19 Compliance Program Considerations
- ✓ Emergency Protocols and Government Actions
- ✓ Waivers
- ✓ Credentialing, Compensation, and Use of Additional Staff
- ✓ Revenue Cycle, Reimbursement, Research
- ✓ Operational Implications of New or Eased Legislation
- ✓ Other Compliance Considerations
- ✓ 340B
- ✓ Coding for COVID-19 Telehealth
- ✓ Information Technology
- ✓ Resources

COVID-19 Compliance Program Considerations

The Compliance Officer in the age of COVID-19...

- Changed and/or relaxed regulatory and legal requirements are creating confusion
- Active participant in decision making regarding the use of various pandemic disaster relief tools
- Must establish a process to report, track, document, and follow-up on all procedural changes
- Serve as the guardian of the crucial repository of information necessary to validate waivers, exceptions, etc.
- Must be the source of regulatory information for the organization

Emergency Protocols and Government Actions

Emergency disaster protocols

- The organization has adequate emergency disaster protocols.
- The organization has reviewed and updated ethics policies and protocols for resource allocation.

FEMA assistance

- The organization has a robust tracking system to account for associated costs to be claimed as extraordinary expenditures for the disaster effort.

Emergency Protocols and Government Actions (cont'd)

The Marshall Plan for healthcare providers

- Ensure the organization has in place a process for submitting an application and supporting documentation requesting funds to build temporary structures, lease properties, medical supplies and equipment, increase workforce and trainings, run emergency operations centers, etc. in order to provide diagnoses, testing, or care for individuals with possible or actual cases of COVID-19.

42 CFR Part 2 provisions of the CARES Act

- The organization has reviewed, revised, and implemented its Substance Use Disorder (SUD) Confidentiality and Disclosure policies for 42 CFR Part 2 program (Part 2) information to meet the amendments provided in the CARES Act and ensure policies align with the HIPAA rules.

Waivers

EMTALA waiver

- The organization has a process for the relocation of individuals for screening at alternative locations as well as the transfer of individuals who have not been stabilized.

HIPAA waiver

- If the disaster protocol has been instituted, does the organization have processes in place to track the timeframe to meet the requirements for the short-term waiver of HIPAA penalties?

Waivers (cont'd)

Telehealth waiver

- *Please see PYA Telehealth thought leadership on the PYA COVID-19 hub for all things telehealth, including Medicare Telehealth Visits, Virtual Check-ins, and E-visits.*

Waivers (cont'd)

Summary of Medicare telehealth services

Type of Service	Service Description	HCPCS/CPT Code	Patient Relationship with Provider
Medicare Telehealth Visits	A visit with a provider that used telecommunication systems between a provider and a patient	**Common telehealth services include:** • **99201-99216** (Office or other outpatient visits) • **G0425-G0427** (Telehealth consultations, emergency department or initial inpatient) • **G0406-G0408** (Follow-up inpatient telehealth consultation furnished to beneficiaries in hospitals or SNFs)	**For new* or established patients** **To the extent the 1135 waiver requires an established relationship, HHS will not conduct audits to ensure such a prior relationship existed for claims submitted during this public health emergency.*
Virtual Check-in	A brief (5 – 10 minutes) check-in with provider via telephone or other telecommunications device to decide whether an office visit or service is needed A remote evaluation of recorded video and/or images submitted by an established patient	• **HCPCS Code G2012** • **HCPCS Code G2010**	**For established patients**
E-visits	A communication between a patient and their provider through an online patient portal	• **99421** • **99422** • **99423** • **G2061** • **G2062** • **G2063**	**For established patients**

Credentialing, Compensation, and Use of Additional Staff

Provider credentialing and licensing

- The organization has a process in place to allow for provisional credentialing to expedite the ability to provide necessary patient care services.

Physician compensation exceptions (Stark)

- The organization has a plan in place to address necessary changes in physician compensation methodology that is based on a productivity-based compensation formula adversely affected by postponement of elective surgeries and decreased outpatient visits.
- Preparing employment agreements and short-term compensation arrangements with physicians who are hired or redeployed to help in the medical response crisis.

Credentialing, Compensation, and Use of Additional Staff (cont'd)

Physician practice enrollment relief

- The organization has a process in place to accommodate provisions for emergency provider enrollment in order to meet patient care needs.

Healthcare workers utilized in alternative positions or unlicensed staff engaged for emergency care delivery

- The organization has a documented process in place to provide for the use of staff in alternative positions, or the use of unlicensed staff as allowed by state statute.

Credentialing, Compensation, and Use of Additional Staff (cont'd)

Patient access staffing and adjusted responsibilities

- The organization has a plan in place to accommodate a dramatic increase in patients entering the facilities, which will require additional patient access staff, technology, personal protective equipment (PPE), and training, as well as patients needing to cancel appointments and procedures.

Telecommuting

- The organization has processes in place that allow non-essential employees to work from home and ensure that confidential and proprietary information is safeguarded.

Revenue Cycle, Reimbursement, and Research

Revenue Cycle: documentation, coding, and billing

- The organization has revenue cycle processes in place to meet the expanded use of telehealth, including appropriate documentation and the accurate use of procedure codes, modifiers, and place of service.
- The organization has processes in place to manage a significant increase in uncompensated care.
- The organization has a process in place to meet CMS requirements to post charges to COVID-19 testing.

Revenue Cycle, Reimbursement, and Research (cont'd)

Reimbursement: accelerated and advance payments program

- The organization has a process in place to evaluate and request accelerated and advance payments from CMS for services provided by hospitals, doctors, durable medical equipment suppliers, and other Medicare Part A and Part B providers.
- CMS fact sheet: https://www.cms.gov/files/document/Accelerated-and-Advanced-Payments-Fact-Sheet.pdf

Relief fund payments

- On Friday, April 10th, HHS began distributing part of the $30B in relief funds to providers. These funds come from a $100 billion appropriation in the CARES Act.
- HHS relief fund payment terms and conditions: https://www.hhs.gov/sites/default/files/relief-fund-payment-terms-and-conditions-04092020.pdf

Revenue Cycle, Reimbursement, and Research (cont'd)

Research and clinical trials

- The organization has a process in place to pause face-to-face research activities except those that affect the safety and well-being of the subjects, or those related to COVID-19.
- The organization has a process in place to review and approve studies and funding related to COVID-19 research.

Image source: Shutterstock

Operational Implications of New or Eased Legislation

Awareness of waivers issued

- The Centers for Medicare & Medicaid Services (CMS) has issued numerous blanket waivers for hospitals and other health care providers.
- These waivers include:
  1. Verbal orders
  2. Discharge planning
  3. Post-acute care patient choice
  4. Use of soft restraints
  5. Completion of medical records
  6. Medical records department organization, form and content of the records, and record retention
  7. Advanced directives
  8. Utilization review condition of participation

Operational Implications of New or Eased Legislation (cont'd)

CMS blanket waivers (cont'd)

9. Nursing care plans
10. Therapeutic diet manual
11. Signature and proof of delivery requirements for Part B drugs and DME
12. Involuntary seclusion
13. CRNA supervision
14. Virtual supervision of residents
15. Supervision for certain hospital outpatient therapeutic services

- CMS COVID-19 Emergency Declaration Blanket Waivers for Health Care Providers: https://www.cms.gov/files/document/summary-covid-19-emergency-declaration-waivers.pdf

Law Enforcement and Theft

Law enforcement: privacy, protection from exposure

- The organization has a process in place to appropriately disclose protected health information (PHI) about an individual who has been infected with or exposed to COVID-19 to law enforcement, paramedics, other first responders, and public health authorities in compliance with the HIPAA Privacy Rule.

Theft of personal protective equipment (PPE)

- To maximize the protection of healthcare workers, the organization must have security processes in place to protect PPE from theft.

Products and Services Fraud

Email and marketing schemes

- The organization has a process in place to detect email and marketing scams related to COVID-19 including:
  - A workforce trained in using caution with email attachments, and avoiding social engineering and phishing scams.
  - The recognition and use of trusted sources, such as government websites, for information, rather than unknown sources purporting to provide financial, product, and services assistance.
  - The verification of authenticity of electronic data received by the organization through use of malware and virus protection software.

Prescription fraud

- The organization has a process in place to monitor and detect prescription drug fraud and diversion of anti-viral drugs associated with the COVID-19 response.

Other Areas to Consider

Vendor due diligence to protect against faulty/inferior/unsafe products and services

- The organization has a process in place to confirm that products offered by vendors are registered with the Food and Drug Administration (FDA).
- The organization has a process in place to document any exceptions made to its vendor policies and purchasing decisions.

PSOs: incident reports of patient/visitor exposure and any associated events

- The organization has a process in place to collect data on incidents related to COVID-19 exposure and treatment in the Patient Safety Evaluation System (PSES) and to identify issues of patient safety and quality improvement to be evaluated and protected under the Patient Safety Act.

Upcoming Information and Guidance

Reimbursement

- Extension for Cost Report Filing

Quality reporting

- Extension in Quality Reporting Deadlines

Image source: Shutterstock

340B Program Update

Review eligible prescriber listings

- Regularly update split billing software and contract pharmacy listings.

Continue to maintain auditable records and supporting program documentation

- HRSA plans to continue audits remotely.
- Abbreviated health records are acceptable.
- Maintain documentation to support relationship between covered entity and providers (including volunteers).
- Ensure policies and procedures incorporate telemedicine practices.

Contact the 340B Prime Vendor Program for assistance with child site registration (case-by-case evaluation)

340B Program Update (cont'd)

Group Purchasing Organization (GPO) prohibition still applies to disproportionate share hospitals, children's hospitals, and freestanding cancer hospitals

- If unavailable at WAC, immediate Office of Pharmacy Affairs notification required for GPO use.
- Report using the HRSA Template Notification Tool.

Be aware of COVID-19 treatment options and associated orphan drug status

Telehealth Coding Update

New definition

- Telecommunications technology with audio and video capabilities that permits real-time interactive communication

Telehealth code list has been expanded

- Eligible provider list has not

Place of Service (POS) codes

- Bill the place of service location where the patient would normally have been seen (absent COVID-19)
- Earlier guidance regarding use of POS 02 has been reversed

Telehealth Coding Update (cont'd)

Include -95 modifier

If hospital outpatient department, bill facility fee

Submit claim to MAC serving provider's location

Telehealth services paid at non-facility rates to compensate practices for telehealth-associated costs

OIG permitting waiver of beneficiary cost-sharing

COVID-19 Cyber Security

The pandemic has created what is known as an Advanced Persistent Threat (APT) to healthcare entities.

APT groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities.

Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised.

COVID-19 Cyber Security (cont'd)

Most common forms of attack

- Phishing, using the subject of coronavirus or COVID-19 as a lure
- Malware distribution, using coronavirus- or COVID-19-themed lures
- Registration of new domain names containing wording related to coronavirus or COVID-19
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure

COVID-19 Phishing

- ✓ To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with "Dr." in their title.
- ✓ In several examples, actors send phishing emails that contain links to a fake email login page.
- ✓ Other emails appear to be from an organization's human resources (HR) department and advise the employee to open the attachment.
- ✓ Malicious file attachments containing malware payloads may be named with coronavirus- or COVID-19-related themes, such as "President discusses budget savings due to coronavirus with Cabinet.rtf."

COVID-19 Phishing

Examples of recent phishing email subject lines include:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your city
- 2019-nCov: Coronavirus outbreak in your city (Emergency)

These emails contain a call to action, encouraging the victim to visit a website that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information, and other personal information.

COVID-19 Phishing for Credentials

A number of cyber criminals have used COVID-19-related phishing to steal user credentials.

- These emails include previously mentioned COVID-19 social engineering techniques, sometimes complemented with urgent language to enhance the lure.
- If the user clicks on the hyperlink, a spoofed login webpage appears that includes a password entry form.
- These spoofed login pages may relate to a wide array of online services including—but not limited to—email services provided by Google or Microsoft, or services accessed via government websites.

COVID-19 Phishing to Deploy Malware

A number of threat actors have used COVID-19-related lures to deploy malware.

- In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked website. When the victim opens the attachment, the malware is executed, compromising the victim's device.
  - Many of these recent attacks deploy the "Agent Tesla" keylogger malware.
  - The email appears to be sent from Dr. Tedros Adhanom Ghebreyesus, Director-General of WHO.
  - This email campaign began on Thursday, March 19, 2020.
- Another similar campaign offers thermometers and face masks to fight the epidemic. The email appears to attach images of these medical products but instead contains a loader for Agent Tesla.

COVID-19 Smishing

Most phishing attempts come by email but federal agencies have observed some attempts to carry out phishing by other means, including text messages (SMS).

Historically, SMS phishing has often used financial incentives—including government payments and rebates (such as a tax rebate)—as part of the lure.

Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages.

Information Technology Considerations

Relaxed HIPAA guidance does not mean unaccountable.

- Yes, using the HIPAA waiver, you can use social video conferencing tools for telehealth visits.
- Covered health care providers **will not be subject to penalties for violations** of the HIPAA Privacy, Security, and Breach Notification Rules **that occur in the good faith provision** of telehealth during the COVID-19 nationwide public health emergency.
- This Notification **does not affect** the application of the HIPAA Rules to **other areas of health care outside of telehealth** during the emergency.
- The Notification of Enforcement Discretion does not have an expiration date. OCR will issue a notice to the public when it is no longer exercising its enforcement discretion based upon the latest facts and circumstances.

Telehealth Technology

Just because you can doesn't mean you should.

- Yes, the federal government has eased restrictions that now allow the use of FaceTime and other platforms.
- However, there are many HIPAA-compliant telehealth solutions that can deployed within hours or days.
- Many of these solutions have full EMR integration options than could be implemented after the COVID-19 influx.

Image source: stevepb for pixnio.com, at https://pixnio.com/objects/tools/hammer-nail-screw-screwdriver-wood-tool-metal

What about tomorrow?

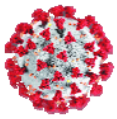
Maybe flattening the curve with COVID-19 has created a reason to strongly consider telehealth, but your decision should be based on much more.

- ✓ Does your telehealth provide easy simple connectivity for all walks of life?
- ✓ Does your telehealth provide apps for Apple, Google, and Microsoft?
- ✓ Does your telehealth provide integration to EMRs?
- ✓ Does your telehealth interact with in-home monitoring devices?
- ✓ Does your telehealth support multiple languages?
- ✓ Does your telehealth meet your state HIPAA and ADA compliance requirements?

Telehealth Landscape Beyond 2020

BEFORE

Before the pandemic, 1 in 10 patients in the US used telehealth, according to a J.D. Power survey from July 2019.



AFTER

One telehealth provider reports appointments are up by 70% since the virus hit the US in January, usage of the app has increased by 158% nationwide, and increased by 650% in Washington State.

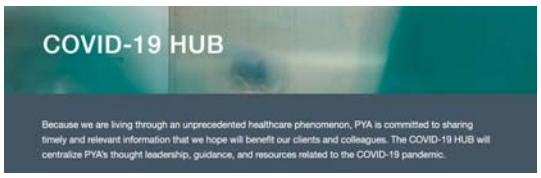
Image source: Shutterstock

Telehealth Landscape Beyond 2020 (cont'd)

- It is said that necessity is the mother of invention, and fewer events fuel necessity more than a disaster.
- Once COVID-19 is behind us, the likelihood that telehealth will go back to its once meager beginnings is doubtful.
- First time telehealth consumers will get a taste of the technology and realize its potential and over time demand better, more accessible and flexible solutions.
- Telehealth can be a major contributor to getting patients back into the care continuum during and after COVID-19.

Image source: Shutterstock

Resources



- Prior webinars on-demand
- PYA thought leadership
- Links to important resources

www.pyapc.com/covid-19-hub/