COSMOS
Navigate the Compliance Universe

Compliance Today - August 2021
Seven compliance hacks for after the COVID-19 pandemic

By Sarah Swank and Charles R. Whipple

Sarah Swank (sswank@nixonpeabody.com) is Counsel in the Washington, DC, office of Nixon Peabody LLP.

Charles R. Whipple (charles.whipple@wellforce.org) is Senior Vice President, Deputy General Counsel, at Wellforce Inc. in Burlington, MA.

At the end of 2019, the Centers for Disease Control and Prevention reported an outbreak of respiratory disease caused by a *novel* (new) coronavirus that was first detected in China. It then was detected in other locations internationally, including in the United States. In response to the pandemic, laws were waived to ensure healthcare providers could prepare and respond to the outbreak. These legal changes created an opportunity for rapid evolution of science, innovation, and technology-driven care models. The pandemic shone a light on discussions regarding social determinants of health and health justice. These changes will likely influence care and payment models, enforcement priorities, and compliance risk beyond the pandemic. Here are seven compliance hacks for staying compliant after the pandemic.

One: Track and ensure PRF compliance

Through the Coronavirus Aid, Relief, and Economic Security (CARES) Act[1] and the Paycheck Protection Program and Health Care Enhancement Act,[2] the federal government allocated payments to be distributed through the Provider Relief Fund (PRF).[3] The intent of the PRF is to support healthcare providers in the battle against the COVID-19 pandemic. Qualified providers of healthcare, services, and support received federal PRF payments for healthcare-related expenses or lost revenue due to COVID-19. These distributions do not need to be repaid, assuming providers comply with the terms and conditions. These obligations include the proper use of the funds, reporting obligations, and return of unused funds to the U.S. Department of Health & Human Services (HHS).

In receiving these funds, the recipient certifies that the payment will only be used to prevent, prepare for, and respond to the coronavirus and that the payment will reimburse the recipient only for healthcare-related expenses or lost revenues that are attributable to the coronavirus. Additionally, recipients must submit all required reports as determined by the secretary of the HHS. The PRF and the terms and conditions for the distributions require that recipients demonstrate that lost revenues and increased expenses are attributable to COVID-19, excluding expenses and losses reimbursed from other sources, or other sources are obligated to reimburse, and exceed total payments from the PRF. PRF payment amounts that have not been fully expended on the combination of healthcare expenses and lost revenues attributable to the coronavirus by the end of the deadline that corresponds to the date the payment was received (or the "Payment Received Period") must be returned to the HHS.

The recipients of PRF payments may be subject to additional auditing to ensure the accuracy of the data submitted to the HHS for payment.[4] Any recipients identified as having provided inaccurate information to the HHS will be subject to payment recoupment and further legal action.[5] All recipients of PRF payments are required to maintain appropriate records and cost documentation to substantiate that recipients used all PRF

payments appropriately.

Noncompliance with any term or condition is grounds for the HHS secretary to direct recoupment of some or all of the payments made. HHS will have significant anti-fraud monitoring of the funds distributed, and the Office of Inspector General (OIG) will provide oversight under the CARES Act to ensure that federal dollars are used appropriately. The recipient of the funds acknowledges in the terms and conditions that any deliberate omission, misrepresentation, or falsification of any information contained in the payment application or future reports may be punishable by criminal, civil, or administrative penalties, including, but not limited to, revocation of Medicare billing privileges; exclusion from federal healthcare programs; and/or the imposition of fines, civil damages, and/or imprisonment.

Use of the PRF should be documented and consistent with the terms and conditions of those funds. No "double-dipping" is allowed, including in conjunction with Paycheck Protection Program loans. Review and audit the documentation related to the use and repayment of unused funds back to the federal government. Retain documentation related to PRF uses and repayments. Report these findings to the board of your organizations to ensure transparency.

Two: Make a list (inventory waivers and enforcement discretion)

On January 31 of last year, the HHS secretary declared a public health emergency (PHE) under section 319 of the Public Health Service Act[6] in response to the spread of the novel coronavirus (SARS-CoV-2), which causes the disease called COVID-19. Less than two months later, then-president of the United States issued the Proclamation on Declaring a National Emergency,[7] and governors across the country issued executive orders declaring a state of emergency due to COVID-19. These declarations led to rapid waivers, changes in law, and federal funding to allow healthcare providers to prepare and respond to the pandemic. State and local governments' waiver authority applies during emergency situations. Reliance on the waivers during the emergency is permitted. Once the emergency is lifted by a particular governmental authority, continued reliance on the waiver creates a compliance problem, since legal support for the waived activity is no longer there.

1135 Waivers

The HHS secretary was authorized to take certain actions based on the president's and the HHS' PHE declaration. These actions triggered waivers authorized under section 1135 of the Social Security Act (1135 waivers) to temporarily waive or modify certain Medicare, Medicaid, State Children's Health Insurance Program, and Health Insurance Portability and Accountability Act (HIPAA) requirements in an emergency area during the emergency period.[8] The 1135 waivers apply to federal law and do not affect state law requirements.

Blanket waivers

Centers for Medicare & Medicaid Services (CMS) can implement specific waivers under its 1135 authority on a "blanket" basis. Under a blanket waiver, CMS determines all similarly situated providers in the emergency area needing such a waiver or modification. Providers can then rely on the waiver without the need to apply for it. It is still recommended to document and track these activities.

Requesting waivers

Healthcare providers may submit requests to operate under the authority of a waiver to the state survey agency or CMS. Generally, providers and suppliers keep careful records of beneficiaries to whom they provide services in order to track that payment is proper and related to the waiver.

Providers are expected to come into compliance with any waived requirements by the end of the PHE. The 1135 waivers "end no later than the termination of the emergency period, or 60 days from the date the waiver or modification is first published unless the Secretary of HHS extends the waiver by notice for additional periods of up to 60 days, up to the end of the emergency period."[9] Examples of 1135 waivers include:

- "Conditions of participation or other certification requirements
- "Program participation and similar requirements
- "Preapproval requirements
- "Requirements that physicians and other health care professionals be licensed in the state in which they are providing services, so long as they have equivalent licensing in another state" (NOTE: state law governs state licensure)
- "Emergency Medical Treatment and Labor Act (EMTALA)" sanctions (A waiver of EMTALA requirements is effective only if actions under the waiver do not discriminate on the basis of a patient's source of payment or ability to pay.)
- "Stark self-referral sanctions
- "Performance deadlines and timetables may be adjusted (but not waived).
- "Limitations on payment" to permit Medicare enrollees to use out-of-network providers in an emergency situation

Once the emergency ends, the waivers end. This means compliance with the law is required.

State executive orders and local laws

Across the country, state chief executives (often the governor) declared state emergencies at different times during the COVID-19 pandemic, invoking powers found in state constitutions and statutes, as well as case law, or implied by the powers assigned to state chief executives to waive state law. State emergency management laws set out how the governor may declare and end a state of emergency. A state may petition the president to declare a major disaster. Federal programs may provide support for major disaster, depending on the scope of the disaster and the type of losses experienced. Waivers during the pandemic have included licensure, telehealth, and other response-related changes. Generally, each state independently declares and ends its emergencies. Counties play a role in public health, data sharing, and other legal consideration during a PHE. Local law should be consulted. For healthcare entities that are located in more than one state, this means following guidance in each state and checking local law requirements. States may be varied in their approach or declaration or end of emergencies. It could mean that the approach for staying compliant within one organization will change state to state.

Three: Focus on digital health and telehealth

The exponential growth in digital and telehealth services by providers adapting to COVID-19 safety protocols has been an overwhelming hit with patients and providers. As PHE declarations that enabled this growth expire, providers need to position themselves to protect and track compliance. A good place to start is to evaluate and understand what types of digital and telehealth services are provided within an organization. It is important to gain an understanding and tracking of the types and locations of telehealth activities that an organization uses to provide guidance and be prepared for when current waivers expire. It is necessary to know where telehealth

services are being provided and where the patients are located when using these services in order to evaluate possible risks. In reviewing the who, what, and where of the telehealth services provided, keep in mind elements such as licensure, corporate practice of medicine, supervisions, and enforcement priorities with new reimbursement.

Licensure

While PHEs are in effect, many jurisdictions have suspended state medical license requirements for telehealth, and meeting those requirements will be necessary after the pandemic. Where the patient is receiving the care generally determines what licenses the provider must hold, and in telehealth, this could be in a different jurisdiction. Review the licensure of providers to determine if they can practice in multiple states. Determine a plan about limiting or thoughtfully expanding telehealth services to patients within your jurisdiction or to a set of providers licensed in additional states. This could be an opportunity to grow your network, but this growth should be done with consideration of compliance with licensure laws. Check both executive orders and state laws, as certain telehealth provisions are being extended by statute.

Corporate practice of medicine and supervision requirements

Another potential area of risk related to the location of patients receiving telehealth services is state-specific regulations on the corporate practice of medicine (CPM). Many states have laws and guidance prohibiting entities from practicing medicine or employing physicians to provide medical services. When providing telehealth or other services across state lines, review the CPM laws in each state and audit and monitor compliance. For example, providers could be delivering telehealth located in a state that permits CPM, while a patient is receiving services while located in a state that prohibits CPM. The cross-state practice could create contracts in the state that require registration as a foreign corporation. In addition, each state has supervision requirements regarding licensed and unlicensed medical professionals. These may differ from state to state. Identify the footprint of the medical professionals and their patients in each state now to understand the compliance risks during and after the pandemic.

Billing, auditing, and monitoring

Federal and commercial payers suspended or adapted billing, coding, and privacy requirements during the PHE. Several jurisdictions have legislated permanent or limited duration rules defining telehealth services and mandating rate equivalency for telehealth services with in-person services. New reimbursement has created an enforcement priority, and audits are on the 2021 OIG Work Plan.[10] Create a revenue cycle process that integrates quality assurance and compliance. Careful monitoring of billing and coding requirements in telehealth is necessary to match dates of service and point of service with services and locations performed to assess compliance. For example, check to see whether both video and audio are required on the date in question or audio connection alone was sufficient. Another tool for auditing coding, depending on the telehealth vendor, is connectivity time stamps for the duration of service provided.

Four: Assess cybersecurity risk

During the pandemic, covered entities and business associates responded to cyber-related security incidents. As part of a compliance program, include an assessment of cybersecurity risks and of the ability to respond to the threat of ransomware. It is likely high. If a cyber-related security incident is identified, the entity should immediately fix any technical or other issues to stop or mitigate the incident. The entity should investigate and report as a breach, if applicable. The HHS Office for Civil Rights presumes all cyber-related security incidents where protected health information (PHE) was accessed, acquired, used, or disclosed are reportable breaches

unless one of the following occurs:

- The information was encrypted by the entity at the time of the incident, or
- The entity determines, through a written risk assessment, that there was a low probability the information was compromised during the breach.[11]

Cybersecurity and prevention should be included in compliance plans as part of the HIPAA Security Rule. The new Stark Law exception[12] and Anti-Kickback Statute safe harbor[13] are in response to the increased number of cybersecurity incidents in healthcare. For example, a hospital could furnish cybersecurity technology to physician practices to reduce harm from cyberthreats to all its systems if the elements of the exception and safe harbor are met. The intent is to protect arrangements for the provision of a wide range of technology donations, which are necessary and used predominately to implement, maintain, or reestablish effective cybersecurity.

Five: Get ready for more value-based compliance

The new[14] value-based payment rules were finalized in the end of 2020.[15] Their aim is to reduce regulatory barriers to care coordination and accelerate the transformation to value-based payments and further coordinated care. A new Stark Law exception and the Anti-Kickback Statute safe harbors regarding value-based entities[16] could open up opportunities outside federal programs, such as the Medicare Shared Savings Program and programs through the CMS Innovation Center. Some wonder if the exception will swallow the rule and allow for broad use, while others wonder if this opens the door to additional government enforcement actions and review. In either event, careful consideration of the use of these new regulations should be taken. Tailor compliance training, auditing, and monitoring to value-based care. Become informed about the role of quality, medical necessity, and utilization review and integrate those activities in the compliance program. Determine the use of data analytics tools to ensure all patients and beneficiaries receive the care they need.

Six: Understand health justice, equity, and inclusion

The impacts of the COVID-19 pandemic highlighted and, in some cases, exacerbated health disparities in both access and delivery of healthcare across the country. The disproportionate impact of COVID-19 on communities of color[17] and those with disabilities[18] include infection rate, access to testing, personal protective equipment, and vaccines as well as to COVID-19 treatment protocols. What is the compliance department's role in helping to address these disparities and create a culturally competent patient care environment? Having a seat at the table during COVID-19 response planning provides an opportunity to educate about a host of recent HHS, Office for Civil Rights, Department of Justice, and Centers for Disease Control and Prevention guidance as well as recent executive orders on ensuring equitable pandemic response and recovery and meaningful access to healthcare.[19] Healthcare providers are creating arrangements with community providers to address social determinants of health such as homelessness, food insecurity, broadband access, and race. These efforts can outlast the pandemic.

Many healthcare organizations are paying significant attention to diversity, equity, and inclusion (DEI) efforts in their patient care and workforce. Compliance officers can reach out to DEI leaders in their organization to offer regulatory support for these efforts. DEI leaders can offer suggestions and support to compliance and legal departments. Whether visitor access issues for patients reliant upon personal caregivers; the need for appropriate signage in multiple languages; or incorporating DEI principles in the crisis standards of care guidelines, decision-making, and execution, compliance professionals and attorneys can provide the regulatory backup to help their organizations meet the needs of diverse and underrepresented populations. Compliance and legal departments can review their own departments and use of outside counsel and consultants regarding DEI.

Seven: Get the board involved

During the pandemic, the myriad guidance and waivers issued by all levels of government gave attorneys and compliance officers a seat at the decision-making table. Compliance departments should not give up this inclusion in a post-COVID-19 environment. There will be a continuing need to update the corporate board through the compliance committee as waivers expire, rule changes potentially become permanent, and new compliance risks develop due to COVID-19. Identification and assessment of these new risks, such as use of different unfamiliar vendors due to supply chain disruptions or heightened scrutiny of the workplace safety personal protective equipment by the Occupational Safety and Health Administration, is part of having an effective compliance program. The compliance committee needs to be updated on these new risks and the auditing and monitoring programs in place for mitigation.

The board and the compliance committee should also be updated on the compliance department's practices that have adapted to remote workforces in healthcare. How has the department adapted by delivering online training, policy reviews, remote employee access and interviews, and desktop reviews? It is necessary to demonstrate that compliance activities and functions have adapted and continue to be effective in the changed work environment. Taking these steps to educate the board will assist with further support from the top of a compliance program.

Stay informed, monitor, and comply

Changes are likely to come fast again. These changes can come in the form of waivers ending, payment reform, public health law, the sprint to care coordination, and the changes needed to adapt to a healthcare system after COVID-19. Make a list, keep informed, and monitor the changes, while informing the board and ensuring robust and integrated compliance activities. Understand how compliance can support and monitor patient-focused activities, such as health justice and equity, public health law, social determinants of health, digital health, and care coordination models that, when done well, put the patient at the center of their own care. The pandemic has brought hardship and created opportunity, and compliance has a role in navigating both.

Takeaways

- Monitor and stay informed of waivers and changes to federal, state, and local law after the public health emergency is lifted. Get your board involved.
- Recipients of Provider Relief Fund grants under the Coronavirus Aid, Relief, and Economic Security Act should track compliance with its use, reporting, and repayment obligations in preparation for possible Office of Inspector General audits and oversight.
- Focus on innovative new models of care as part of compliance programs, including the use of digital health, telehealth, and value-based care.
- Cybersecurity preparation and response efforts were highlighted by the new Stark Law exception and Anti-Kickback Statute safe harbors.
- Focus on diversity, inclusion, and equity in your compliance program and staff.

1 Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, 134 Stat. 281 (2020).
2 Paycheck Protection Program and Health Care Enhancement Act, Pub. L. No. 116-139, 134 Stat. 620 (2020).
3 "CARES Act Provider Relief Fund," U.S. Department of Health & Human Services, last reviewed January 21, 2021, https://bit.ly/36nqH9F.

4 "Audit of CARES Act Provider Relief Funds—Distribution of $50 Billion to Health Care Providers," Office of Inspector General, U.S. Department of Health & Human Services, accessed June 14, 2021, https://bit.ly/3aiuQPh.
5 "Provider Relief Fund General Information (FAQs)," U.S. Department of Health & Human Services, accessed June 14, 2021, https://bit.ly/2RXnJGe.
6 U.S. Department of Health & Human Services, "Secretary Azar Declares Public Health Emergency for United States for 2019 Novel Coronavirus," news release, January 31, 2020, https://bit.ly/3iLWvxn.
7 Donald J. Trump, "Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak," March 13, 2020, https://bit.ly/3zup88e.
8 42 U.S.C. § 1320b-5 .
9 "1135 Waivers," Centers for Medicare & Medicaid Services, last modified January 11, 2021, https://go.cms.gov/3wo7Fwd.
10 "Work Plan," Office of Inspector General, U.S. Department of Health & Human Services, accessed June 14, 2021, https://bit.ly/3cWW0d0.
11 U.S. Department of Health & Human Services Office for Civil Rights, "My entity just experienced a cyber-attack! What do we do now? A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)," accessed June 18, 2021, https://bit.ly/3zCdSGM.
12 42 C.F.R. § 411.357(bb) .
13 42 C.F.R. § 1001.952(jj) .
14 Centers for Medicare & Medicaid Services, "CMS Announces Historic Changes to Physician Self-Referral Regulations," news release, November 20, 2020, https://go.cms.gov/3iToVW6.
15 Medicare and State Health Care Programs: Fraud and Abuse; Revisions to Safe Harbors Under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements, 85 Fed. Reg. 77,684 (December 2, 2020) , https://bit.ly/2L6TXet.
16 42 C.F.R. §§ 411.357(aa), 1001.952(ee) -(gg).
17 American Hospital Association, "The Disproportionate Impact of COVID-19 on Communities of Color," statement for the Committee on Ways and Means of the U.S. House of Representatives, May 27, 2020, https://bit.ly/3virkMA.
18 Stephen Frost, "Deadly Discrimination: The Forgotten Impact Of Covid-19 On People With Disabilities," *Forbes*, July 6, 2020, https://bit.ly/3gR7YZW.
19 "Civil Rights and COVID-19," U.S. Department of Health & Human Services, last reviewed June 11, 2021, https://bit.ly/2TW5MZi.