HCCA™
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

APRIL 2018

A smooth transition

an interview with
Gerry Zack
Incoming CEO
SCCE & HCCA

ARTICLES

Compliance
TODAY

EXECUTIVE EDITORS: Gerry Zack, CCEP, Incoming CEO, HCCA
gerry.zack@corporatecompliance.org

Roy Snell, CHC, CCEP-F, CEO, HCCA
roy.snell@corporatecompliance.org

NEWS AND STORY EDITOR/ADVERTISING: Margaret R. Dragon
781.593.4924, margaret.dragon@corporatecompliance.org

COPY EDITOR: Patricia Mees, CHC, CCEP, 888.580.8373
patricia.mees@corporatecompliance.org

DESIGN & LAYOUT: Pete Swanson, 888.580.8373
pete.swanson@corporatecompliance.org

PROOFREADER: Bill Anholzer, 888.580.8373
bill.anholzer@corporatecompliance.org

PHOTOS ON FRONT COVER & PAGE 16: Bethany Meister

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to Compliance Today, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Copyright © 2018 Health Care Compliance Association. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means without prior written consent of HCCA. For Advertising rates, call Margaret Dragon at 781.593.4924. Send press releases to M. Dragon, 41 Valley Rd, Nahant, MA 01908. Opinions expressed are not those of this publication or HCCA. Mention of products and services does not constitute endorsement. Neither HCCA nor *CT* is engaged in rendering legal or other professional services. If such assistance is needed, readers should consult professional counsel or other professional advisors for specific legal or ethical questions.

VOLUME 20, ISSUE 4

by John P. Benson, JD, AHFI, CFE

Telemedicine, Part 2: Navigating the steps to the practice of telehealth care

- Licensure requirements are evolving to streamline the practice of telehealth.
- Telehealth care's exponential growth rate creates a frenzied, reactive regulatory and administrative response.
- Enrollment regulations and policies are in perpetual flux.
- Communication of PHI/PII must be trusted, authenticated, and encrypted for HIPAA compliance.
- Telehealth care creates a powerful convergence of data, knowledge, and technology with a potential for delivering greater efficiencies.

John P. Benson *(john@verisys.com) is Chief Executive Officer and Co-Founder of Verisys Corporation in Alexandria, VA.*

Part 1 of this article appeared in the January 2017 issue of Compliance Today.

Part 1 of this article series covered the origin and drivers of telehealth and telemedicine. In summary, the evolution of telemedicine has been positively demonstrated to improve patient outcomes, lower federal healthcare spending, expand patient access to quality care, manage the unbalanced ratio of limited healthcare providers to an expanding patient population, and reduce hospital ER/ED wait times and loads.

Benson

For the balance of this article, the use of the term *telehealth care* will refer to both telemedicine (the remote experience of clinical healthcare) and telehealth (monitoring, training, and other support mechanisms through a remote protocol). In either case, the web, telephony, secure servers, and apps are in use.

This rapidly expanding platform of healthcare introduces complexities that could implode the hospital administrative system because of the exponential growth of not only the practice of telehealth care, but also the use of locum tenens. As the use of telehealth care evolves, scalability and security will be the prevailing considerations as the massive Baby Boom generation reaches Medicare age.

Foundational concepts

Before we look at the steps that enable the practice of telehealth care, the following paragraphs describe foundational concepts.

Connectivity between providers and patients

Telehealth care enables providers and patients to connect nationwide or globally. Patients can seek and receive care from specialists no matter where the provider chooses to practice, connecting patients with the best providers for his/her individual conditions without the added time, risk, or expense of travel.

Connectivity between providers and between providers and academics/researchers

Sharing knowledge contributes to higher assurances of favorable outcomes as well as accelerating research by removing the barriers of institutional silos. For those who participate in collectively treating challenging cases and contributing to research, relevant data is correlated to a greater universe and applied more quickly to patients from diverse populations.

Increasing the level of transparency of providers in the system and enhancing consumer choice

Telehealth care and the regulatory requirements of licensing, credentialing, privileging, enrollment, and compliance enhance transparency as providers navigate through the required steps to practice in multiple institutions and states. Although those who have something to hide will likely self-select out and choose not to practice telemedicine for fear of exposure, for those who do participate, the steps create an added gatekeeping layer. Telehealth, being web or app enabled for consumers, will create a level of transparency that will assist in consumer choice — not necessarily referral-based or network-based, but based on the provider with the best credentials, outcomes, and pricing, or a market-driven combination of the three.

Steps to compliant telehealth services

A number of steps are required in order to practice telehealth care: (1) licensing, (2) credentialing, (3) privileging, (4) enrollment, and (5) Health Insurance Portability and Accountability (HIPAA) privacy compliance.

Step 1: Licensing

Obtaining a license to practice medicine is the first step in gatekeeping and making sure that professionals are adequately trained to deliver the services permitted under the scope of their license. Each state's licensing board implements the regulations or administrative codes of its state's legislative action. In order to legally practice medicine in multiple states, providers must be licensed according to the unique laws, regulations, and administrative codes of the respective state medical boards in every state in which they wish to practice. The only regulatory burden imposed on the practice of medicine from a federal level is prescriptive authority (i.e.; the ability to distribute or prescribe controlled substances).

If a specialist desires to extend their practice nationwide via telehealth, the specialist could fork out in excess of $50,000 for license fees and countless hours completing some 35–60 pages of various applications per state. The cumbersome reality of practicing medicine nationwide could hinder practitioners from offering services across multiple state lines; however, there are actions in motion to remedy the time-consuming and tedious process, while preserving competency requirements, compliance, and transparency.

A report published by the Federation of State Medical Boards portrays the variety of laws that affect healthcare licensure. For instance, the medical boards of 48 states, plus the District of Columbia, Puerto Rico, and the Virgin Islands, require that providers of telemedicine be fully licensed in the state in which the patient is located; whereas the medical boards of 15 states issue what is termed a special purpose license, a telemedicine license or certificate, or a license to practice medicine across state lines to providers of telehealth care. The medical boards of four states require providers to register if he or she wishes to practice across state lines.[1]

A coalition of states have put together a streamlined process for gaining reciprocal licensing that spans state borders. It's called the Interstate Medical Licensure Compact. Currently, 22 states have passed legislation adopting the Compact, and other states are moving the legislation forward.[2] The Compact works to simplify licensure requirements among member states, making it easier for providers to practice in multiple states. The Compact comes to the table with two core ideas: (1) increase access to healthcare for individuals in rural as well as underserved areas; and (2) break down the silos of license status by sharing investigative and disciplinary information, resulting in a reduction of patient harm, risk, and fraud.

Step 2: Credentialing

Credentialing is a process intended to certify a provider's competence by researching all related education, training, experience, competence, and licensure. Depending on the state, the payer, and the institution, providers may likely be required to be credentialed with each hospital in which they practice. The Joint Commission (TJC), DNV GL (a hospital accreditation group), Healthcare Facilities Accreditation Program (HFAP), the National Committee for Quality Assurance (NCQA), the Utilization Review Accreditation Commission (URAC), the Centers for Medicare & Medicaid Services (CMS), and commercial payers have a weigh-in on credentialing requirements. Credentialing may not be mandatory in cases such as with private-pay patients, or consultation where the exchange is between physicians while care of the patient remains with the originating physician, or in an instance where practitioners are not required to be credentialed.[3]

The credentialing process is conducted by the Medical Staff Services office whose team is typically overloaded with its own provider population's processes and requirements. The added workload of credentialing telehealth care providers as well as locum tenens practitioners can be unpredictable and unwieldy. To better understand the varying stages of credentialing, one can look at credentialing as a three-stage process consisting of (1) data collection and verification, (2) review, and (3) recommendation and final action.

The added workload of credentialing telehealth care providers as well as locum tenens practitioners can be unpredictable and unwieldy.

The first stage is slowed by duplication of efforts. The task of data collection and verification usually happens in several different departments, information is not shared, and each department within a hospital often uses different data sources as well as its own vendor or staff for primary-source verifications.

Until the digital paradigm is fully and interchangeably adopted and a central source of locked, verified data informs across multiple departments and institutions, the medical staff services team painstakingly researches, requests, waits, and verifies primary-source static data such as a physician's medical school diploma. As it is, each time a provider requests to be credentialed with an additional hospital, another medical staff officer reaches out—again—to that same medical school for information that has already been provided and verified. And that is only one of a dozen or so items that are static, yet go through the same primary-source verification process repeatedly.

The other two stages are unique to each hospital and involve department chairs, committees, and the board. Policy, bylaws, and procedure either elongate Stages 2 and 3 into 120 days or more, or compress it to a few days by fine-tuning the process of the credentialing board.

Conceptually, the reason to credential a provider is to protect the patient. This is the process where you would find out if that provider has any exclusions, debarments, or disciplinary actions pending, current, or in the past. This process also verifies education, special training, past practice history, and much more. It is where the Medical Staff Services office vets a provider to granular detail so they don't accidentally hire a non-licensed or unqualified provider, a sex offender, or an identity thief.

The practical reason for credentialing is to be eligible to receive reimbursement from federally funded programs such as Medicare and Medicaid. CMS governs whether hospitals are worthy of receiving reimbursements based on compliance with federal regulatory standards.[4] CMS has approved some standard-setting bodies and organizations to certify a hospital as eligible to receive federal reimbursements. The standards are designed to circle back to quality care and patient safety.

With the emergence of telehealth care, both CMS and some standard-setting bodies have worked to develop credentialing-by-proxy processes where treatment hospitals can communicate with and accept credentialing from the originating-site hospitals. In many cases, this means that smaller hospitals can "borrow" the services of specialists from larger hospitals and accept the credentialing of those larger hospitals without jeopardizing their own standing, as long as a specific set of requirements are met.

The list of requirements provided on the Center for Connected Health Policy's website currently include:

- There must be a written agreement between the two parties;
- The distant-site hospital is a Medicare-participating hospital or telemedicine entity;
- The telehealth provider is privileged at the distant-site hospital;
- A current list of the telehealth provider's privileges is given to the originating-site hospital;
- The telehealth provider holds a license issued or is recognized by the state in which the originating-site hospital is located;
- The originating-site hospital has an internal review of the telehealth provider's performance and provides this information to the distant-site hospital; and
- The originating-site hospital must inform the distant-site hospital of all adverse events and complaints regarding the services provided by the telehealth provider.[5]

This list must also fit within the distant-site hospital's bylaws and policies and provides some abbreviation of a full credentialing process, but still requires engagement from the Medical Staff Services office to verify and execute the requirements.

Step 3: Privileging

In addition to provider credentialing, organizations must perform a process of privileging for their providers. Although providers are often educated and licensed to perform a broad range of procedures and provide a wide variety of services, many providers specialize their work to a much smaller subset of their possibilities. For this reason, healthcare entities must assess the individual skill set of each provider and approve that provider for the various procedures and services offered by the healthcare entity. Without the "privilege" to perform a specific procedure, a provider who might be fully qualified cannot perform the procedure.

Privileging is informed by CMS guidelines,[6] but the process is created and governed by the policies and bylaws of individual hospitals. Processes could include:

- obtaining primary-source verification from a certifying educational institution,
- referral from a supervising provider who holds the requested privileges,
- direct proctoring among other processes that are particular to the type of environment,
- level of risk,
- specific experience vs. training, and
- other considered circumstances.

As with credentialing, CMS and some standard-setting bodies have released standards to enable a privilege-by-proxy agreement between healthcare entities.

Determining the privileging of a provider is a time-intensive effort that is required for accreditation. As with credentialing, CMS and some standard-setting bodies have released standards to enable a privilege-by-proxy agreement between healthcare entities. By taking advantage of these standards, hospitals can reduce the administrative burden of accessing specialists via telehealth methodologies.[7]

Step 4: Enrollment

Enrollment is a key component to receiving payment, and it has as many faces as the payers, the institutions, and the states one chooses to engage with. Typically, a practitioner will enroll with several dozen insurance payers, and each enrollment process takes several months. Payers can require a different sequence in which a hospital must credential, privilege, and enroll. At times, payer requirements can stack the lead times, making for an unmanageable distance between application and compliant practice, and reimbursement.

In order for Medicaid to reimburse covered services, the engagement of telehealth care in providing those covered services must adhere to the federal requirements of efficiency, economy, and quality of care. States can choose to reimburse for telehealth care services in the same way they reimburse for in-person visits and incorporate the additional details (e.g., a facility fee, the providers at both the distant and originating facilities, equipment, and transmission fees) within their standard submission for reimbursement. If a state bills and seeks reimbursement differently than for in-person visits and care, those states will submit a separate State Plan Amendment (SPA). In both cases, request for reimbursement must stay within the Federal Upper Limits of the Affordable Care Act.[8]

Private payers are not required by federal law to provide coverage for any type of telehealth care, but states may require coverage and payment for certain types of telehealth care.

The Public Health Institute's Center for Connected Health Policy covers telehealth-related laws, regulations, and Medicaid programs for all 50 states plus the District of Columbia and publishes an annual report called *State Telehealth Laws and Reimbursement Policies*.[9]

In the most recent report released in October 2017, it notes that 48 states, on behalf of Medicaid fee-for-service policies, reimburse for live video but not necessarily store-and-forward or remote patient monitoring. Store-and-forward involves the acquisition of clinical information (e.g., image, sound, or data) that is subsequently forwarded to another site for clinical evaluation. Fifteen states include store-and-forward in their Medicaid program policies, and some are requiring private payers to also cover store-and-forward; 21 states reimburse for remote patient monitoring; and nine state Medicaid programs reimburse for all three with restrictions.

Other significant trends include counting the home as an eligible origination site and allowing a virtual initial visit, thus not requiring an in-person consultation to establish a practitioner relationship with the patient prior to providing telehealth care services. Among the variables that states treat uniquely are the location, type of institution, condition being treated, provider type, and whether it is physician-to-physician or physician-to-patient, among others.

To effectively manage revenue flow and ensure timely coverage and payment, it is recommended to be familiar with each respective state law as well as private and federal payer reimbursement policies for each instance of billing. As regulatory requirements proliferate, it is essential to stay current with laws and recommendations so as to avoid compliance violations and the possibility of making false claims.

Step 5: HIPAA privacy compliance

At large, a hospital's compliance program is designed to ensure that a hospital conforms to state and federal law, state and private payer healthcare requirements, and the internally decided ethical and business policies of a hospital.[10] The compliance item most germane to telehealth care is the Health Insurance Portability and Accountability Act (HIPAA) in the effort to protect a patient's privacy throughout the entire life cycle of a remote communication process. Navigating the path of HIPAA compliance through telehealth technology is a new challenge of providers and institutions engaged in telemedicine.[11]

Of the steps mentioned in this article, compliance is the most complex and robust. Where licensing, credentialing, and privileging occur at periodic intervals, compliance is a requirement for each and every interaction a provider has with a patient, collaborator, vendor, referral, or lab. Telehealth care introduces a wide variety of ways in which providers may unknowingly violate HIPAA through misinterpretation or accidental oversight of compliance regulations in every act of communication, documentation, and storage of protected health information (PHI) as well as personally identifiable information (PII).[12]

For example, simply using a commercially available video-chat service to talk with a patient, or sending a text or email to follow up could cause a breach of HIPAA. How? HIPAA dictates that all PHI must be encrypted and protected so that only very specific persons can access it. This includes maintaining encryption and data control during all phases of the information's life cycle—including storage.

When you send an email, it is housed on a server somewhere. Is that server appropriately encrypted? Ditto with the string of electrons that transmits information for a video chat. That information has to pass through a server on its way between provider and patient computers and could be stored as a backup along the way. If that server isn't appropriately secured and encrypted, it could be possible to unknowingly transmit PHI via unsecured, HIPAA-noncompliant methods. This is especially true in the case of email or text messages, which patients are likely to store *and view* on servers and platforms without the appropriate security protocols.

One solution is to use a secure messaging platform on the provider's network that creates an encrypted, secure connection between patient and provider, as well as provider and provider, at each contact. In the case of messaging, this typically involves storing all information on the provider's network and granting access to the patient and other providers as needed, effectively restricting the information according to HIPAA and state requirements.

Providers would be compelled to create a secure portal to safely communicate to colleagues, labs, and patients; however, where colleagues, labs, and patients may have relationships with multiple providers, they would have user names and logins for each provider.

The future begs for an anti-competitive platform standard that meets HIPAA compliance as well as each state law, and is engineered with level Tier 3+ security measures. Currently, many telehealth app developers do not consider themselves a covered entity or business associate, and therefore, the app is not subject to HIPAA. Many states have enacted privacy and security laws that would govern the use of an app and make an app subject to oversight by the Federal Trade Commission.

Conclusion

For some time, bringing patient records into an electronic format has been an initiative, but with the advent of telehealth care, the electronic health record (EHR); the electronic medical record (EMR); and now, electronic, secure, web-based provider credentialing/privileging/enrollment profiles may become the industry standard.

Technology plays a large part in each and every aspect. With licensing, credentialing, and privileging, industrywide use of comprehensive, current, accurate data; automation; and secure, centralized records would eliminate the duplication of the same efforts by myriad state boards and hospitals.

Telehealth care provides a wider net of quality healthcare to a broader population and, additionally, creates a convergence of knowledge and data through the use of secure technology. Because of the components that require sharing information, silos are dissolving. The proliferation of relevant data enhances research; informs best practices and education; expands patient access to quality healthcare; provides data points for analytics; quickly exposes those who pose risk to patient care; and detects systemic fraud, waste, and abuse.

[1] Federation of State Medical Boards, Telemedicine Policies, Board by Board Overview (a state-by-state summary of requirements to practice telemedicine). Available at http://bit.ly/2G37XiJ

[2] Interstate Medical Licensure Compact. Available at http://www.imlcc.org

[3] Telehealth Resource Centers: "Credentialing and Licensing." Available at http://bit.ly/2DVU9Vi

[4] CMS Quality, Safety &Oversight – Certification and Compliance. Available at http://go.cms.gov/2FHr7cx

[5] Center for Connected Health Policy: Credentialing and Privileging (provides suggested guidelines for a proxy process). Available at http://bit.ly/2HMWILF

[6] CMS Memorandum to State Survey Agency Directors regarding "Centers for Medicare & Medicaid (CMS) Requirements for Hospital Medical Staff Privileging" November 12, 2004. Available at http://go.cms.gov/2EzIhJH

[7] 76 Fed. Reg. 25,550 (May 5, 2011), Medicare and Medicaid Programs: Changes Affecting Hospital and Critical Access Hospital Conditions of Participation: Telemedicine Credentialing and Privileging; Final Rule. Available at http://bit.ly/2nGfqLU

[8] Medicaid.gov: Affordable Care Act - Federal Upper Limit. Available at http://bit.ly/2E0c5SD

[9] Center for Connected Health Policy, The National Telehealth Policy Resource Center: State Telehealth Laws and Reimbursement Policies, Fall 2017. Available at http://bit.ly/2EBHvvM

[10] 63 Fed. Reg. 8,987 (Feb. 23, 1998), Publication of the OIG Compliance Program Guidance for Hospitals. Available at http://1.usa.gov/1cedJaK

[11] Telehealth Resource Centers: HIPAA and Telehealth. Available at http://bit.ly/2EDOHHX

[12] Health IT.gov: Privacy & Security, Integrating Privacy & Security Into Your Practice. Available at http://bit.ly/2E6VlIT