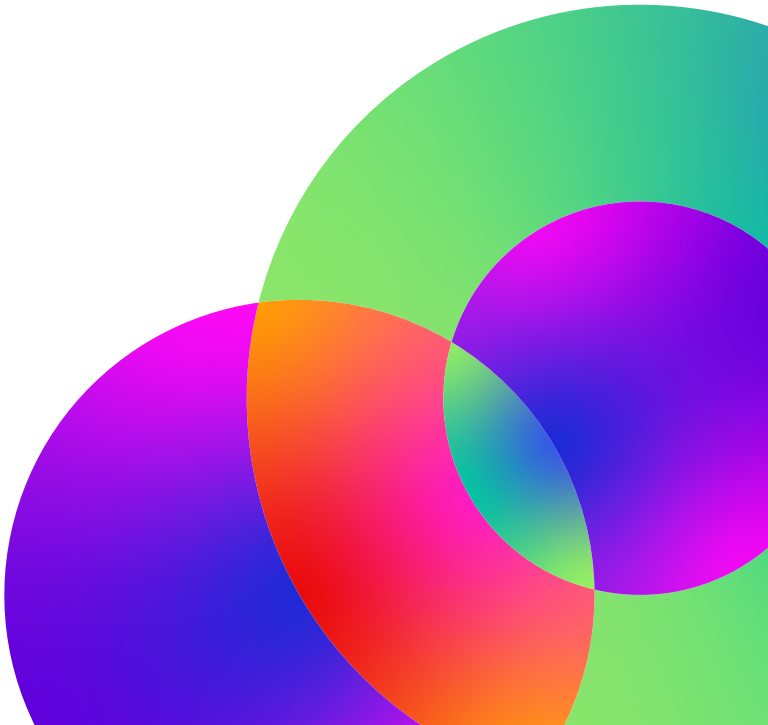
Best Practices for a Remote CVO Workforce



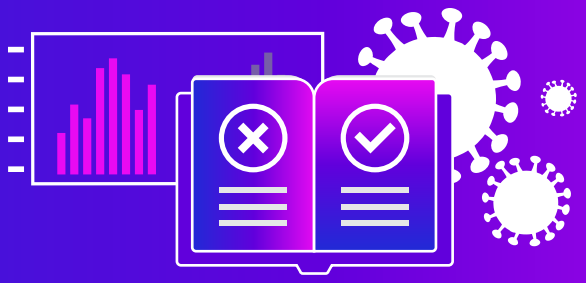
symplr

Overview

Regardless of a credentialing verification organization's (CVO's) physical location and the provider data management methods and technologies it uses, the hospital maintains ultimate responsibility for the work performed.

CVOs exist to help healthcare systems verify licensed medical professionals' qualifications and enroll providers into payer health plans. They do so by accepting delegated responsibility to assess clinicians' backgrounds, identify gaps, and report the findings—either as a contracted third party or as an internal centralized credentialing function.

As a result, hospitals must ensure alignment when using a CVO that employs or contracts with remote staff.



Lessons from COVID-19

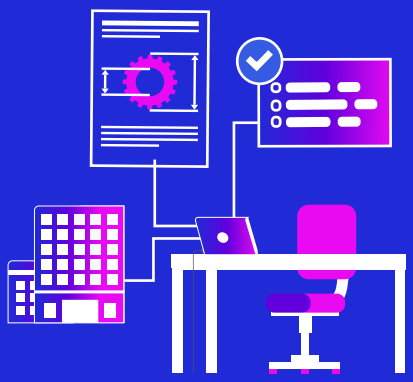
Technology has long enabled remote work setups, but the COVID-19 pandemic brought unanticipated lockdowns and restricted hospital access. Considered essential, many medical staff services departments, CVOs, and administrative offices performing primary source verification (PSV), credentialing, and privileging quickly went virtual out of necessity.

Even before COVID-19, however, credentialing and payer enrollment (PE) roles in CVOs were viable candidates for successful remote technology setups. Against the backdrop of telehealth's rapid expansion and predictions about tomorrow's healthcare-delivery sites lacking a physical location, it's easy to imagine provider data management roles shifting primarily to remote.

A paradigm change about which roles lend themselves to being conducted from a virtual office appears to have already begun. For example, a March 20, 2020 survey of 317 CFOs and finance leaders by Gartner, Inc., showed that one-fourth of respondents said they will move at least 20% of their onsite employees to permanent remote positions. In the same survey, 22% polled said they already made cost reductions to real estate or plan to soon.

Allowing CVO staff to work remotely is, of course, attractive financially in terms of reduced overhead. But a Harvard Business School study across multiple professions also found advantages may extend to increased productivity of workers. Still other studies tout higher employee morale, recruiting advantages, and a positive environmental impact.

For some roles like PSV or enrollment in a CVO, there may be no going back to the pre-Coronavirus norm of commuting daily to a brick and mortar hospital or healthcare administrative office site. Yet there are key considerations to ensure your remote CVO staff—or those of your third-party CVO—are aligned.



Why build an alignment strategy for remote CVOs?

In any outsourced work arrangement, common data management and technology challenges exist and must be addressed to ensure success. Factor in hastily constructed remote workforce setups, especially amid COVID-19, and the healthcare system's exposure to risk increases. After all, a CVO mines and manages the provider data used to make essential decisions that affect:

- Regulatory compliance and patient safety
- Successful reimbursement
- Provider data security
- Practitioner satisfaction
- Health plan inclusion and patient access to care
- Organizational reputation

Whether the relationship with a CVO using remote staff is years old or brand new, it's never too late to examine key data management and technology factors. symplrCVO has extensive experience with remote CVO workforce management and was among the first provider data management software companies to establish a virtual CVO workforce. As a result, we offer best practice tips for successful data management when using credentialing and PE specialists who telecommute for a CVO.

Implement these strategies when using internal remote CVO staff, or seek these characteristics when partnering with a third-party CVO that employs telecommuting staff.

Ensure provider data security

Healthcare organizations go to great lengths to protect patient data, but provider data requires safeguarding, too. Ensuring data security is the single biggest challenge when credentialing or enrollment is conducted remotely. Specific points of vulnerability exist in every system. For CVOs, those key areas include data or document source, viewing authorization, transmission method security, and data or document storage (i.e., long-term control).

A CVO's work is focused on PSV, the act of going directly to the source of the credential or the institution that issued the document or verifying data through a designated equivalent source. As a result, the remote staffer or CVO organization secures access to other organizations' hosted data. However, in addition to collecting providers' data for initial appointment, enrollment, recredentialing, and keeping practitioners "par" (i.e., participating) on health plan panels, the data is used elsewhere. For example, quality initiatives such as shared savings programs, merit-based incentives, and provider performance management require provider information. In the age of data breaches, it's important for remote staff to understand where the confidentiality lines are drawn.

Best practice preventive measures to take when using remote CVO staff include the use of:

- A virtual private network (VPN) routed through the internet from the company's server or a third-party VPN service to the remote CVO staff.
- Multi-factor authentication, whereby the remote CVO staff are granted access only after successfully presenting two or more "keys" to an authentication mechanism (i.e., log-in credentials).
- Data loss prevention software that detects and prevents potential data breaches and allows a network administrator to control what data remote workers can upload or download transfer, and to whom.

Involve your IT department

All roads will lead back to your IT department regarding the setup of and data security for remote CVO staff. If you're embarking on the use of a remote CVO workforce, seek technology experts' help from the outset. If your virtual CVO is up and running, schedule regular check-ins with IT to relay challenges and any ongoing technical issues. The IT team keeps hardware and software up to date, but must be aware of your CVO-related specifications. They can suggest options and best practice solutions you haven't thought about, and security will always be atop IT's agenda.

Learn to speak IT's language:

"Cloud" refers to software and/or software as a service (i.e., SaaS) running on the internet (public or private), instead of on a local area network. Business applications delivered via SaaS skip the complicated installations, and the software vendor hosts and maintains the servers, databases, and the code that comprise the application.

Browser is the program used to access the web (e.g., Google's Chrome, Mozilla's Firefox, Microsoft's Edge and Explorer, and Apple's Safari). Browser choice can affect the way information is viewed and tasks are performed, especially when using sites where provider data is catalogued or uploaded via online applications. Keep browser type(s) in mind when collaborating with and training remote staff.
Cookies are messages that web servers pass to a web browser when internet sites are visited, and can affect performance. Train remote staff about how cookies can affect their ability to upload and download data.

Use a single source of truth database

Use of a single, shared, full-spectrum credentialing database is ideal to foster efficiency and security for remote CVO staff, regardless of physical location. A shared platform that is the single source of truth enables the medical staff office (MSO) or health plan to outsource all or a portion of the credentialing or provider enrollment process to the CVO while still maintaining control of the data.

A cloud-based solution that the MSO and CVO can access from any location or computer and that manages data across the entire lifecycle of a practitioner fosters the ability to:

- Communicate more effectively in sharing data with all relevant parties
- Ensure data integrity and transparency
- Demonstrate accountability for large volumes of traceable data
- Prepare for inevitable growth

Short of using a singular, shared solution, follow these best practices for data alignment:
Speak the same language: Ensure that remote staff use the same actions and data types to communicate in your data environment.
Keep remote staff focused: Use reports as regular updates to eliminate unnecessary back-and-forth email communication or extraneous meetings.
Consider creating a shared, secure portal: Provides remote CVO staff with the policies, tools, best practices, and compliance guidance they need to access regularly.

Track procedures and KPIs

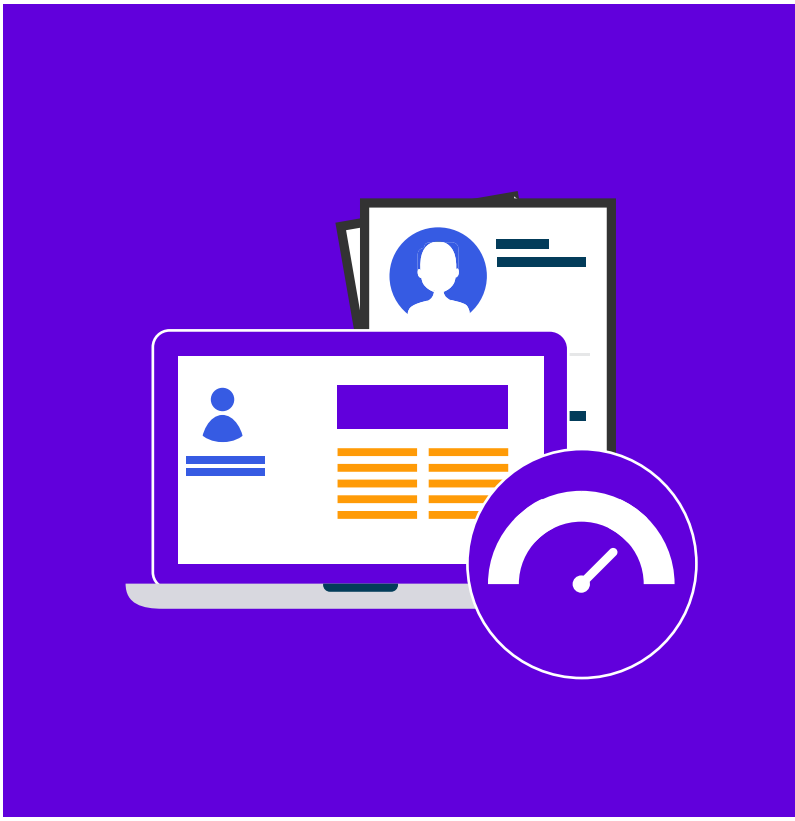
Understanding the procedures that the CVO executes on your behalf sounds straightforward. But often, neither internal nor third-party CVOs outline detail-oriented policies and procedures for remote staff until a problem's identified. It's a time-consuming but necessary first step to gather such information. Document all systems (technological or otherwise) remote staff use to collect, manage, and disseminate data and documents. This exercise most often uncovers that members of the CVO and medical staff team are duplicating efforts.

Reporting on key performance indicators not only shows ROI, but also demonstrates the need for additional resources if needed. Best practice tips for procedure mapping and benchmarking include the following:

- Develop one process to be used by both the CVO and MSO: Eliminate duplication and create a clear and clean path for all remote staff to follow, and train them on it.
- To gauge individual performance metrics for remote staff: Measure multiple data points along the life cycle of enrollment and credentialing to pinpoint problems or delays.
- Track the efficiency and effectiveness of the remote CVO's processes in measurable terms and dollars and cents. The configuration and reporting functions you might need for a remote workforce get more complex as you determine whether credentialing/privileging, enrollment, and quality/competency assessment all share the same provider data management source.

CVOs perform critical business processes that can and often do affect the organization's bottom line. They require significant technological resources to maintain modern, efficient processes regardless of their physical location.

symplrCVO is the NCQA-certified, trusted expert credentialing verification service for healthcare and insurance providers, with a team that's ready to support you, whatever your needs.



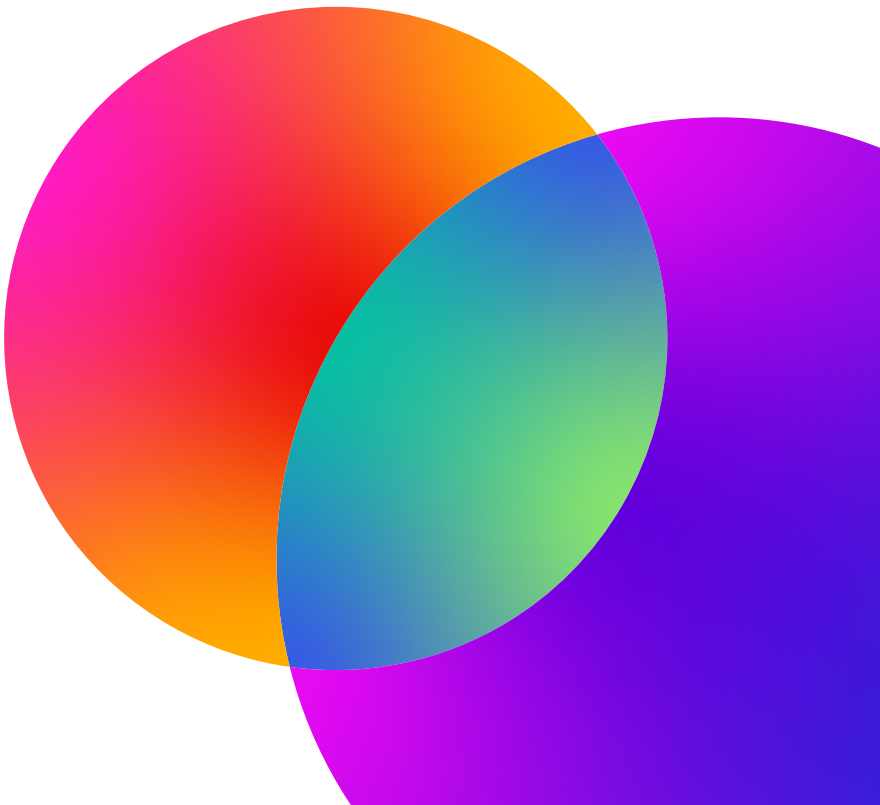
About symplr

symplr's comprehensive healthcare operations solutions, anchored in governance, risk management, and compliance, enables our enterprise customers to efficiently navigate the unique complexities of integrating critical business operations in healthcare.

For over 30 years, our customers trust our expertise and depend on our provider data management, workforce and talent management, contract management, spend management, access management, and compliance, quality, safety solutions to help drive better operations for better outcomes.

As your trusted guide, we follow a proven approach to help you achieve your organization's priority outcomes by breaking down silos, optimizing processes, and improving operational systems.

Learn how at www.symplr.com.



symplr