FOUR TIPS: THE INVISIBLE IMPACT OF CREDENTIALING

TIP 2 OF 4

Newport Credentialing
SOLUTIONS™

TIP: 2

MAKE SURE ALL DATA IS PROTECTED – NOT JUST PHI

NewportCredentialing SOLUTIONS™

Make Sure All Data is Protected – Not Just PHI.

More than two decades ago, the Health Insurance Portability and Accountability Act (HIPAA) was signed into law. One of its most significant provisions was to create a standard method of protecting patient data, regardless of where it resides. In 2000 additional safeguards were put in place and Protected Health Information (PHI) became the responsibility of everyone in the healthcare sector. As a result, compliance programs and business associate agreements were created and rolled out to ensure anyone who could be exposed to PHI respected its discreet characteristics and would take necessary steps to protect patient privacy.

While a tremendous amount of work has been done to ensure data security in the healthcare industry, there is still much more to be done. As news of data breaches top headlines, hospitals and other healthcare organizations are stepping up their data security efforts. IT staff are working diligently to ensure EHR systems, accounting systems, and other patient-related software systems are secure. Meanwhile, with the focus primarily on patient information, one-off areas like credentialing and enrollment are being overlooked which is putting many providers sensitive information at risk.

Because provider data is not PHI, it is not subjected to the rigorous protection standards demanded by HIPAA. While many organizations have internal compliance programs designed to shield employees, vendors, and providers from unexpected data breaches, provider data is all too commonly found on loosely protected Excel spreadsheets, Word documents, and in unsecured email transmissions. When this information sits unprotected on an individual desktop, thumb drive, or network server, it becomes vulnerable to hackers and unauthorized individuals (some of whose intentions may be less than honorable).

Tip 2

SECURE CREDENTIALING & PROVIDER DATA

CENTRALIZE ALL CREDENTIALING DATA

Eliminate paper documentation and one-off locations for storing provider data. Provider credentialing and enrollment data should be stored in a protected central repository and made available only to individuals with a need to access it.

CONTROL DATA ACCESS

Ensure policies and procedures are put in place for storing, accessing and sharing provider data. Policies should be detailed and require hard passwords to access any provider data and prohibit users from sharing log in ID's or passwords.

BACK UP YOUR DATA

Take steps to ensure that provider credentialing data is included as part of your organization's data compliance and disaster recovery programs. Co-location backups and off-site storage are sound processes to protect against data loss.

MONITOR DATA ACCESS AND USAGE

Make sure all transmission of provider data is secure. This may mean using a secure portal instead of email to transmit information to plans. IT audit trails should be implemented to track the "who, what, when, and where" each time data is accessed.

LET'S GET STARTED

With these best practices in place, change your provider enrollment department from a cost center to a revenue generator.

To learn more, contact Newport Credentialing Solutions at info@newportcredentialing.com or 516.593.1380.

Phone: 516.593.1380
Email: info@newportcredentialing.com

NewportCredentialing
SOLUTIONS™