Protecting Patients

Your doctor knows just about every quantifiable thing about you. Think about it. Height? Check. Birthday? Check. Credit card information? Check. Social security number? Home address? That time you broke your arm in the third grade? You get the idea. This plethora of information is exactly why those handling your medical information, from your local doctor all the way to the insurance company, are such viable targets for cyber criminals. It’s a one-stop shop for fraudsters.

This is, of course, no secret. Cyberattacks have drifted in and out of headlines for a few years now, but according to a KPMG survey, health care organizations are woefully underprepared to defend your data. A remarkable four out of five health care

executives report that the private information they store has been compromised at least once. Further, only 53 percent of providers and 66 percent of payers consider themselves ready to defend against attacks.

So what's the hold up? That answer might be as straightforward as it seems. First, health care organizations are just that: focused on care. There is, in many cases, a lack of focus on security when there is so much to be done in terms of patient care. There are other factors at play as well, namely the federal government. Health care is one of the most regulated industries in the country, and in some cases, that regulation might be preventing the implementation of security best practices. According to a representative from KPMG, some providers still rely on Windows 7 and XP because certain updates to their technology would require Food & Drug Administration approval. Yikes.

It's clear that more emphasis has to be placed on securing medical information, especially as the prevalence of electronic health records grows. But where to start? It seems that the issue has to be dealt with from two ends. To begin, lawmakers must consider updating regulations that are stalling

progress. At the same time, health care executives need to prioritize security and instill it in their organizations from

the top down.

At CNSI, we're working hard to provide health care solutions that fully comply with security standards. From solutions such as the cloud to mobile applications which provide patients with information while ensuring that security requirements like authentication, authorization and identity management are well covered.

As our Medicaid Enterprise Systems Conference keynote speaker Frank Abagnale put it, "Security is everyone's responsibility, and we must close the doors before criminals find their way in." We couldn't agree more.

How can the industry do a better job protecting medical information? Tell us your thoughts by commenting or finding us on Twitter @CNSICorp.