Managing information technology services across the Sharp Community Medical Group network of more than 200 primary care physicians and 500 specialists based in San Diego, California, we often guide clinicians on how to balance convenience and ease-of-use with security and regulatory compliance requirements.

Sharp Community Medical Group addresses the increased use of smartphones, tablets, and other mobile devices.

Our providers are hard-working, budget-conscious physicians driven by a shared passion for patient care. They are being asked to do more with less—to improve the quality of care while reducing costs. More and more, they are looking to technology for solutions. They believe technology should enhance—but never impede—the patient care process. They also understand the need to comply with the Health Insurance Portability and Accountability Act (HIPAA), safeguard privacy, and secure protected health information (PHI). Our solutions, therefore, must improve the quality of care and reduce costs while safeguarding patient information.

In our role, we share this sentiment and make every effort to accommodate the needs of our providers. However, we also remain diligent with respect to security and compliance to help Sharp Community Medical Group clinicians meet the aims of HIPAA privacy and security rules: that patient information is readily available in appropriate care settings, but secured against inappropriate use.

In November 2012, these issues rose to the fore during an education campaign to help our providers understand Meaningful Use (MU) and the requirements necessary to qualify for incentives. As part of this process, we reminded our clinicians about their HIPAA obligations and the potential impact to patients if PHI is exposed, even when the violation is unintentional.

One particular issue we addressed was the increased use of smartphones, tablets, and other mobile devices that we were seeing across our network. These devices deliver fast, convenient communication that busy clinicians need as they move to and from their individual practices into large hospital venues. However, they also introduce potential risks that we alerted our providers to.

What we learned during this process is that many providers are looking for quicker, more convenient ways to communicate with colleagues. They were considering using their smartphones, but most providers did not have the necessary policies in place to properly regulate the use of mobile devices and text messaging, creating potentially significant security and compliance gaps.

The Paging Problem

Contacting and conferring with fellow clinicians typically involved using pagers, waiting for callbacks, and exchanging voicemails before finally connecting with a colleague to discuss a particular patient case. What we heard from our providers was that this was inefficient...
and detracted from patient care. Time that could be spent interacting with and treating patients was instead wasted dealing with outdated communication technologies.

To remedy the situation, many providers started using the same methods of communication they use every day in their personal lives—smartphones and text messaging. This instant, two-way means of communicating and collaborating is far more efficient than paging a colleague and waiting for a callback.

Unbeknownst to our clinicians, however, is that the native Short Message Service (SMS) text messaging they were considering is not encrypted, so sharing PHI could expose sensitive patient data and violate HIPAA regulations. We understood their intention—our clinicians were simply looking for improvements in providing patients with timely, efficient care.

The situation we found ourselves in is not uncommon in health care. In fact, a study from Imprivata from 2013 revealed some interesting findings about the productivity and economic impact that the use of pagers and other traditional forms of communication has on the healthcare industry.¹

The study surveyed 577 U.S. healthcare professionals, including doctors, nurses, administrators, and IT practitioners. Respondents overwhelmingly—and given our experience, not surprisingly—agreed that using deficient communications tools decreases productivity and limits the time doctors spend with patients, which also translates to significant industrywide financial loss (see Figure 1).

For example, according to the study, the average clinician wastes more than 45 minutes each day due to the use of outdated communication technologies. The primary reasons cited include the inefficiency of pagers, the inadequacy of email, and the inability to use text messaging.

From a care perspective, the survey found that clinicians spend only about 27 minutes of every hour with patients, with the remaining time spent either communicating or collaborating with colleagues or using electronic medical records (EMRs) and other clinical IT systems.

This also impacts a health system’s bottom line—the time wasted by clinicians dealing with communications deficiencies costs the average U.S. hospital more than $900,000 per year, translating to an industrywide loss of more than $5.1 billion annually.²

**FIGURE 1**

**Average Physician Time Wasted with Outdated Communications Technologies**

<table>
<thead>
<tr>
<th>REASONS CITED?</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inefficiency of pagers</td>
<td>52%</td>
</tr>
<tr>
<td>Lack of WiFi</td>
<td>39%</td>
</tr>
<tr>
<td>Inefficiency of e-mail</td>
<td>38%</td>
</tr>
<tr>
<td>Texting not allowed</td>
<td>36%</td>
</tr>
</tbody>
</table>

**WASTED TIME...**

The average clinician wastes more than 45 minutes per day due to outdated communication technologies...

**A Grudging Agreement**

When we informed our providers that using SMS text messaging to communicate PHI was a potential compliance violation, they grudgingly agreed not to use it but stressed the need for a more efficient, convenient, and HIPAA-compliant solution for communicating and collaborating with colleagues.

Given that many of our clinicians were already gravitating toward the use of text messaging as their preferred method of communication, we focused our search on finding a secure texting solution that met HIPAA requirements, but also one that met our providers’ specific clinical requirements to share text and picture messages with colleagues.

For example, we needed a solution that offered a robust directory that includes the names, roles, specialties, and any published phone numbers of both ambulatory and hospitalist providers, allowing them to quickly and conveniently identify the desired contact. This was essential to meet our providers’ primary requirement—increased efficiency in the communication process for timely care coordination.

Also, because our providers are constantly monitoring their patients as they move across the continuum of care within the network, they interact and collaborate with colleagues in varied organizations. Therefore, we sought a solution that enables access to multiple organization directories and allows our providers to securely communicate with colleagues across varied settings.

Additionally, to optimize the value of text messaging as a real-time communication solution, we wanted to enable our providers to request a callback within the text message itself. This eliminates the tedious process of paging, which requires clinicians to find a call list, locate a phone, send a page, and wait by the phone until the return phone call comes back.

At the same time, our solution needed to employ the most effective methods in securing PHI: for ex-
ample, the use of strong encryption while a message is in transit as well as when the information is at rest on the server or on a provider’s smartphone. It was also critical that the vendor we selected be willing to sign an HIPAA Business Associate Agreement to ensure that our providers would be protected if any PHI was exposed as a result of using a third-party text message solution.

After an extensive review of the many emerging text messaging applications and products available, we elected to deploy Imprivata Cortext, an HIPAA-compliant secure text messaging solution that satisfies all of our clinical and IT security requirements.

When we introduced the solution to our providers, they immediately recognized it as a welcome improvement in the clinical communication and collaboration process. Today, our providers benefit from a fast, convenient, and easy-to-use communications solution without fear of exposing PHI and jeopardizing patient privacy. This helps clinicians remain focused on patient care, allowing them to deliver timely, cost-effective, and informed diagnoses and guidance to patients.

Pain Points Alleviated

The results we experienced in collaboratively rolling out a secure text messaging solution illustrate how advances in IT help clinicians work efficiently and cost-effectively for the betterment of patient care without sacrificing security or HIPAA compliance requirements. Working together to understand the IT needs of our providers and the specific pain points they were experiencing, we were able to offer a solution that aligns with our collective objectives.

This is one of many examples where technology can alleviate the tensions that often exist between clinicians—who want access to whatever technologies best serve patient care—and the IT staff, which is tasked with meeting HIPAA compliance requirements and safeguarding PHI. We advise others experiencing similar challenges to develop a process for identifying challenges within the organization and collaborating closely with clinicians to design an IT communications plan that satisfies the needs of all stakeholders.

References

2. Ibid.

Chuck Deckert is vice president, health information technology solutions, and David Porter is technical project manager at Sharp Community Medical Group.