

HIPAA regulation: The challenge of integrating compliance and patient care

January 2016

Contents

Introduction	3
HIPAA's "technology neutral" structure creates opportunity and challenge	3
Compliance can pave the way for meaningful use	4
Clinician communication varies and is expanding into new modes	6
Current strategies leave room for improvement	8
Unified care team collaboration platforms are underutilized	10
Sources	11

perfectserve.com | 866.844.5484 | @PerfectServe

Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.

©2016 PerfectServe, Inc. All rights reserved. PerfectServe® is a registered trademark and PerfectServe Synchrony™ and Problem Solved™ are trademarks of PerfectServe, Inc.

Introduction

The expansion of communication technology within healthcare organizations involves great promise and great risk.

Keeping information flowing and the right people connected at the right time creates potential for more effective patient care and population health management.

But a greater number of moving parts also means greater risk. With personal health data moving at greater frequency through an increasing variety of digital channels, the complexity of communicating in a secure manner as mandated by HIPAA regulations is on the rise, as is the risk to the confidentiality and integrity of patient data.

While the complexities of compliance—and the penalties for breaches—are daunting, the true challenge of HIPAA regulations for healthcare organizations is to integrate security compliance into their overall goals of providing high-quality individual patient care and improving population health management. Secure communication is mandatory and vital for patient confidentiality, but it is not intended to be a barrier to high-quality, efficient care.

In fact, HIPAA regulations are intended to mesh with and provide a foundation for the kind of proper, efficient exchange of information that grounds new models of collaborative care. HIPAA's core mandate is threefold: confidentiality, integrity *and availability*. Getting HIPAA compliance right means greater communication and, ultimately, a positive impact on patient care. To make this happen, healthcare organizations need to assess how their members communicate, building compliance into the model in ways that enhance workflow. Finding secure ways to encourage and streamline the flow of information can align the need for HIPAA compliance with the trend toward greater collaboration and the goal of better patient care.

HIPAA's "technology neutral" structure creates opportunity and challenge

HIPAA Security Rule regulations require all covered entities to subject their policies, procedures and technical infrastructure to ongoing risk analysis and to implement a comprehensive strategy to ensure confidentiality, integrity and availability of electronic personal health information (ePHI), however and whenever it is stored or communicated.

Any method of communicating ePHI must, under the Security Rule, meet technical standards for Access Controls, Audit Controls, Integrity, Person or Entity Authentication and Transmission Security.

However, the law does not regulate or provide guidance on the specific technologies health organizations may use to store and communicate ePHI. The law is intentionally technology neutral; it does not prescribe or restrict storage or communication methods—it only mandates that they meet security standards in these areas.

For healthcare organizations, this is good news. The law does not restrict methods of communication or specify use of technologies that are continually becoming outdated. This encourages flexibility and innovation, as new ways of communicating can fuel new ways of coordinating care.

The law permits individual organizations to assess and adopt the technologies they feel will best serve their overall goals and structure.

However, this flexibility also comes at a price. The burden falls on healthcare organizations to structure their communication strategies, proactively vetting and choosing technologies that fit in with overall healthcare goals. They also must ensure that every aspect of the way they handle sensitive personal health information is secure—every method of communication, every device, every software platform, every network. As methods of communication change and proliferate, the task becomes larger and more complex, requiring greater strategic planning and more organizational resources.

Compliance can
pave the way for
meaningful use

Facing this challenge, organizations may simply focus on or feel overwhelmed by the technical complexity of bringing their communications into compliance—losing sight of a larger potential. The flexibility within the Security Rule is essential to achieving its third core tenet: *availability* of information. The ability to store and transmit data securely means that it *can be shared* among all those on the care team—keeping the right people informed in a timely manner. According to the Department of Health and Human Services, “permitting the appropriate access and use of that information, ultimately promotes the use of electronic health information in the industry—an important goal

of HIPAA.”¹ Security compliance actually encourages the exchange of information that can bring about greater efficiencies and better outcomes in our healthcare model.

The intent to dovetail compliance with coordination improvements is exemplified in the push to encourage “meaningful use” of electronic health records (EHRs). Starting in 2011, the Centers for Medicare & Medicaid Services (CMS) began administering an incentive program to promote the transition to electronic health record systems. The goals of this program are not only to solidify patient data security but also to enhance the ability of healthcare organizations to use that data in *meaningful ways*. Securing data in compliance with HIPAA regulation through an EHR can not only “maintain privacy and security of patient health information,” but also enable healthcare organizations to “improve quality, safety, [and] efficiency, and reduce health disparities; engage patients and family; [and] improve care coordination, and population and public health.”²

While related to a single aspect (EHRs) of the data storage and communication technologies covered by the Security Rule, the meaningful use program crystalizes the potential that secure communication systems hold. The ability to store and communicate data securely means the ability to use that data responsibly and creatively to improve delivery of quality healthcare for individual patients and system-wide. The stages of a meaningful use EHR program defined by CMS [Table 1] show how such technical advances could have far-reaching effects on many aspects of our healthcare system, from public health initiatives to greater engagement of patients and families in their own care.

Ultimately, it is hoped that meaningful use of HIPAA-compliant technologies will result in:

- Better clinical outcomes
- Improved population health outcomes
- Increased transparency and efficiency
- Empowered individuals
- More robust research data on health systems³

This vision depends, however, on systems that can meet the technical

security standards required by HIPAA, and streamline workflow and improve clinician communication.

Table 1


Source: www.healthit.gov/providers-professionals/how-attain-meaningful-use

Stage 1: Meaningful use criteria focus on:	Stage 2: Meaningful use criteria focus on:	Stage 3: Meaningful use criteria focus on:
Electronically capturing health information in a standardized format	More rigorous health information exchange (HIE)	Improving quality, safety and efficiency, leading to improved health outcomes
Using that information to track key clinical conditions	Increased requirements for e-prescribing and incorporating lab results	Decision support for national high-priority conditions
Communicating that information for care coordination processes	Electronic transmission of patient care summaries across multiple settings	Patient access to self-management tools
Initiating the reporting of clinical quality measures and public health information	More patient-controlled data	Access to comprehensive patient data through patient-centered HIE
Using information to engage patients and their families in their care		Improving population health

Clinician communication varies and is expanding into new modes

The challenge of finding the best HIPAA-compliant communication strategies is particularly pressing as, in the search to improve patient care through clinician coordination and patient communication, healthcare organizations are increasingly relying on a complex, *often ad hoc*, array of technologies and communication platforms. The current workflow and communication model is high-volume and intricate.

Clinicians coordinate care within networks and with external partners using a host of devices and applications, generating a high



volume of contacts. In an analysis of PerfectServe data from three hospitals, representing an aggregate of 774 beds and 54,000 annual admissions, clinicians initiated more than 680,000 calls and messages to approximately 900 physicians annually. In a recent online study conducted by Harris Poll on behalf of PerfectServe among various healthcare professionals, data further reveals the intricacy of the system. Phone calls, text messages, email, EHRs, locating an individual for a face-to-face conversation—all are used with varying frequency according to the preferences of the individual clinician, the type and complexity of information sought, and whether the recipient of the message is within the clinician’s organization or is an outside partner.⁴ Recent data also indicates that multiple platforms rather than a unified system is the norm: in a study of nearly one thousand healthcare professionals, 69% indicate their organization uses multiple applications and technologies for secure communication.⁵ An organization must account for all of these methods in assessing risk to patient data and must ensure that all methods meet the security standards set by HIPAA.

Additionally, health organizations are using an ever broader and more technically complex system of communications to optimize population health management [**Table 2**]. These methods serve to improve quality and availability of care, but also rely on the transmission of patient data. More contacts and more methods of communication between clinicians and their patients mean more points at which that health data could be vulnerable and more systems to bring into compliance.

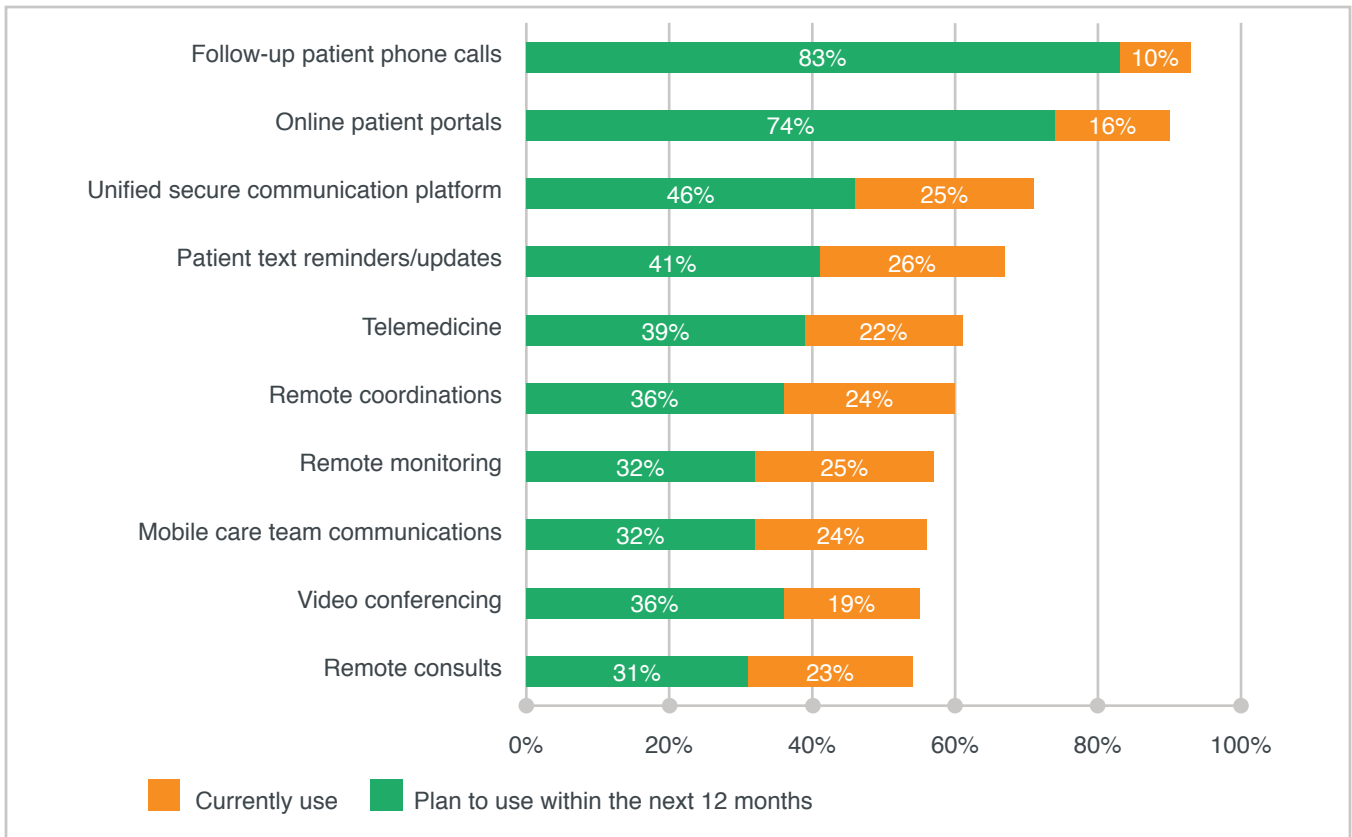


Table 2

Source: Harris Poll, April 2015

Q920: Which of the following technologies does your organization currently use or plan to use within the next 12 months to optimize population health management?

Base: All Qualified Respondents (n=955)

Current strategies leave room for improvement

Thus, the reality of how clinicians communicate creates a maze of communication technologies for healthcare organizations to submit to risk analysis and bring up to security standards. As healthcare organizations continue to embrace collaboration and the breadth of communication technologies that make it possible, HIPAA compliance will only become more complex.

How successful are health organizations in meeting this challenge?

Studies show that while most healthcare organizations are prioritizing data security, current strategies leave significant frustration and room for improvement both in compliance strategies themselves and in the integration of compliance with improved workflow.

Organizations have HIPAA-compliance risk mitigation strategies in place and many are working to improve them in the wake of recent data breaches. A recent survey shows the vast majority work in a group that

84%

Indicate their health organization has a risk mitigation plan for HIPAA

46%

Say their health organization has instituted security measures in response to news of 2014 healthcare data breaches

61%

Agree that HIPAA regulations pose an obstacle to efficient communication and collaboration within the care team

has an official risk mitigation strategy, and 4 out of 5 (83%) believe that secure communication is a top priority for their organization; nearly half indicate their group has made changes to that plan in light of recent prominent data breaches.⁶

But the solutions most rely on are not ideal. Despite the overall emphasis on security and level of organizational commitment, frustration and dissatisfaction exist with methods of secure communication, patient data is still being transmitted in unsecure ways, and barriers to communication are impacting patient care. The recent survey indicates that:

- For most, the strategies necessary for compliance have not been neatly integrated into their workflow: **61% feel that HIPAA regulations pose an obstacle** to efficient communications and collaboration within their care team.
- Compliance is a priority, but the tools available are not always up to the task: **nearly 3 in 10 (29%) are dissatisfied with the secure communication technology** in their organization's current strategy.
- Despite efforts, the failure of healthcare organizations to create a unified, complete system is the primary source of frustration: **the most commonly cited reasons for dissatisfaction** are the variance in communication technologies used by different members of the organization (68%) and the failure to have secure communication accessible to all members of the organization (55%). **Lack of uniformity in the system and universal access to all team members** are much stronger factors in dissatisfaction even than technical deficiencies such as outdated, unreliable software or programs that are complicated to use.
- When a web of disparate technologies is in place and not everyone is included in the same system of communication, collaboration and efficient patient care face a hurdle: **7 in 10 clinicians (69%) indicate that patient care is often delayed** while they wait for information about a patient.⁷

The gaps in an organization's strategy can also lead to failures in compliance, leaving patient health information vulnerable to exposure or corruption. Despite the emphasis on communication security and

the strategies in place, 13% of healthcare professionals admit that, in order to facilitate patient care, they have sent patient health information through unsecure text or voice messages with their personal smart phone in the past year, and 21% acknowledge having received unsecure communications from colleagues via the same manner for this purpose.⁸

While breaches occur for many reasons, the majority can be traced to inadequately planned processes and tools organizations develop internally to manage this complicated landscape. A 2015 Ponemon Institute study of ePHI security breaches indicates that the underlying causes of these breakdowns are most often an ad hoc process (34%) or a manual process or tool developed by the organization itself (27%). Incidents traced to an automated process or third-party software occur at a much lower rate (13%).⁹

Unified care team collaboration platforms are underutilized

For healthcare organizations that are increasingly embracing more collaborative care models and the technologies that make care more accessible and efficient, the answer to HIPAA compliance must focus simultaneously on data *security and availability*. In a world of rapidly expanding communication methods and applications, points at which the communication model can be streamlined as well as secured can reduce the burden of ongoing risk management on organizations.

A unified care team collaboration platform can help organizations simplify their risk management strategy, relying on a single integrated system rather than tracking and juggling multiple systems. It can also ameliorate the two main causes of dissatisfaction with secure communication within healthcare organizations: not all members using the same technologies and not all members having access to secure communication technology.

However, this strategy is not being as widely implemented as it could be, with nearly 7 in 10 (69%) healthcare professionals reporting that their organization deals with multiple technologies rather than one unified platform.

As organizations review and work to improve their risk management strategies, a unified communications platform can be an important piece of the move toward integrating HIPAA compliance with the best patient care and population health management possible.

Sources


1. "Security 101 for Covered Entities." HIPAA Security Series: Volume 2, Paper 1. Department of Health and Human Services. 2007. Available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>.
2. <https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives>. Accessed December 7, 2015.
3. <https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives>. Accessed December 7, 2015.
4. PerfectServe Survey Results, April 2015. Harris Poll.

The PerfectServe survey was conducted online by Harris Poll on behalf of PerfectServe between February 12 and March 6, 2015. The research was conducted among 955 medical professionals in the following occupations: hospitalist (n=150), primary care physician in an office (n=150), specialist physician in a hospital (n=102), specialist physician in an office (n=101), hospital administrator (n=170), office manager/practice administrator* (n=81), nurse in a hospital (n=101) and case manager (n=100). Office-based respondents work in an office with 25 or more physicians. Hospital-based respondents work in a hospital with 200 or more beds. Physician respondents are duly licensed in the state where they practice. Data were not weighted and are only representative of those who completed the survey.

*Nine office managers/practice administrators work in an office with fewer than 25 physicians.

When referring to this study, "clinicians" indicates a subset of respondents excluding administrators. The subset includes hospitalist (n=150); PCP office (n=150); specialty physician, hospital (n=102); specialty physician, office (n=101); nurse, hospital (n=101); and case manager (n=100), for a total base of n=704.

5. PerfectServe Survey Results, April 2015. Harris Poll.
6. PerfectServe Survey Results, April 2015. Harris Poll.
7. PerfectServe Survey Results, April 2015. Harris Poll.

- 
8. PerfectServe Survey Results, April 2015. Harris Poll.
 9. Ponemon Institute, Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2015. Available at <http://www.ponemon.org/library/fifth-annual-benchmark-study-on-privacy-security-of-healthcare-data>.