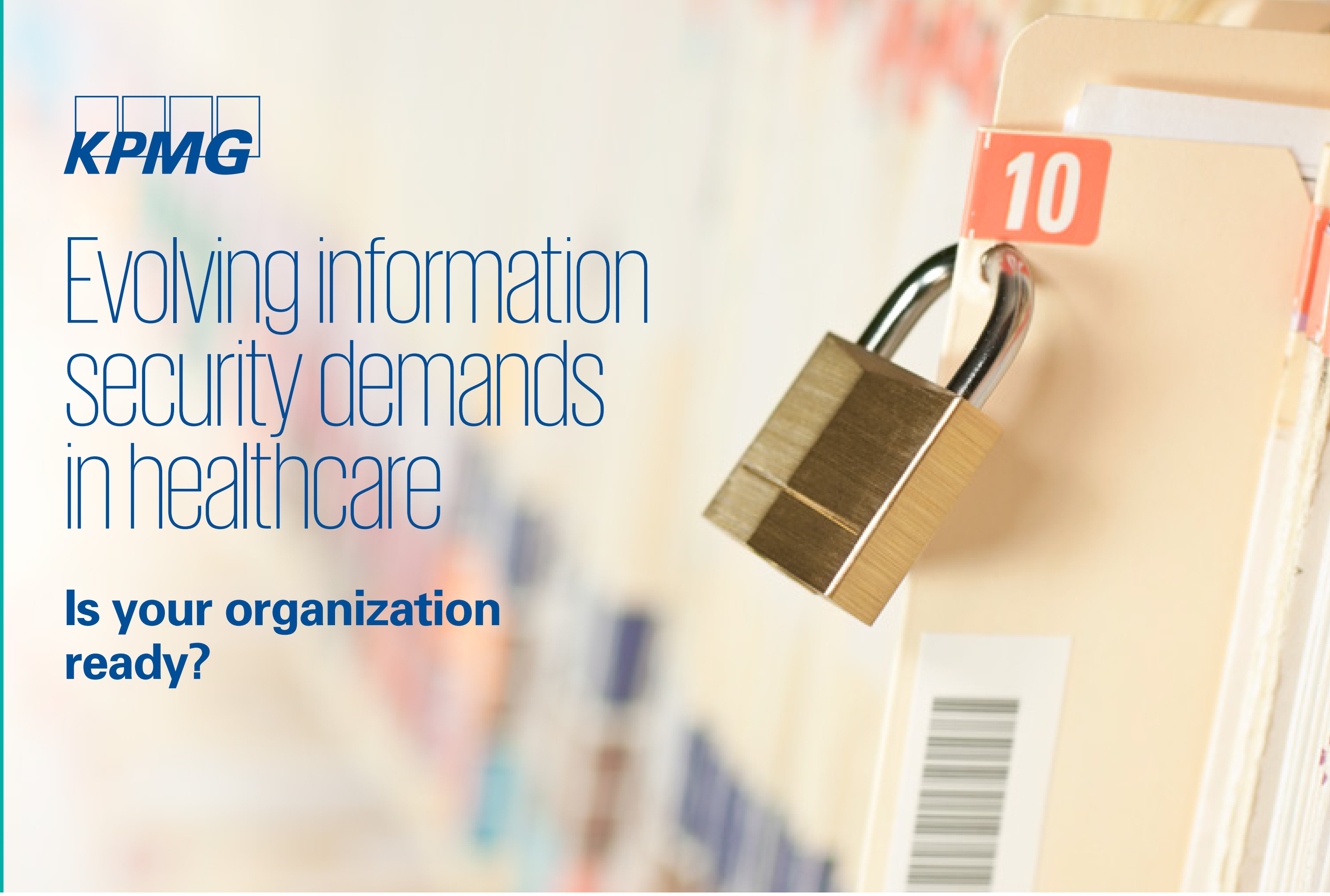
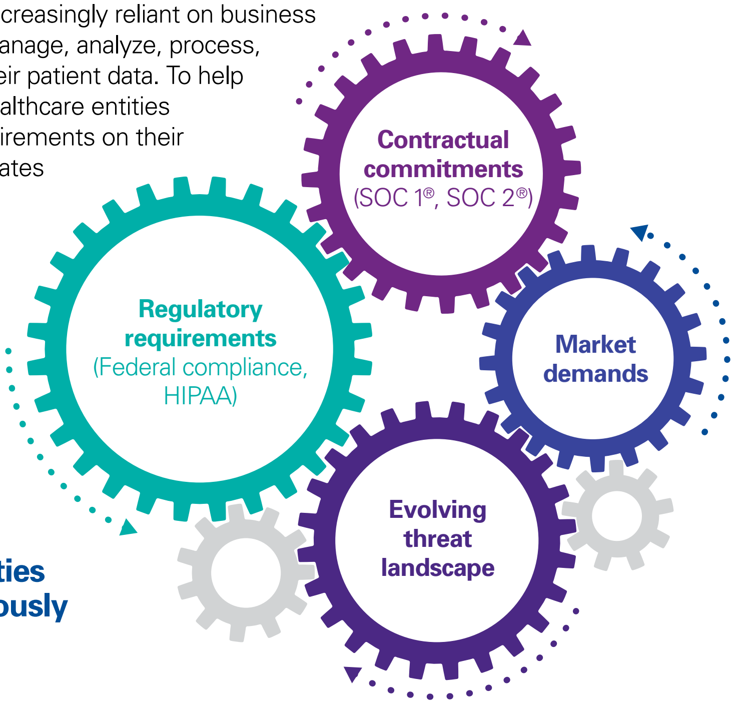


KPMG

# Evolving information security demands in healthcare

## Is your organization ready?

In the wake of highly publicized, hard-hitting security events and elevated regulatory pressure, healthcare entities are increasing scrutiny on their business associates—those entities who create, receive, maintain or transmit protected health information (PHI) on behalf of a covered entity. In today's technologically driven and rapidly converging business environment, healthcare organizations have become increasingly reliant on business associates to manage, analyze, process, and interpret their patient data. To help manage risk, healthcare entities are placing requirements on their business associates to demonstrate their ability to secure PHI.

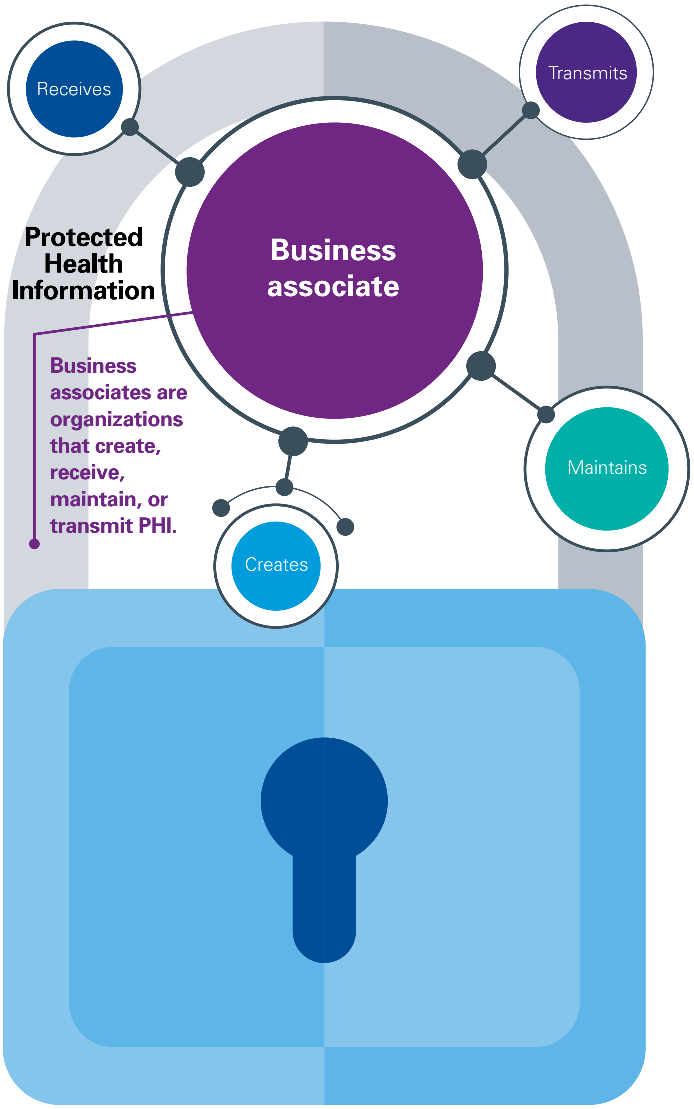

Contractual commitments (SOC 1®, SOC 2®)
Regulatory requirements (Federal compliance, HIPAA)
Market demands
Evolving threat landscape

**Healthcare companies' responsibilities are continuously changing.**

**To help manage risk, healthcare entities are placing requirements on their business associates to demonstrate their ability to secure PHI.**

A **business associate** is a person or organization that performs certain functions and activities or provides services on behalf of a covered entity (a healthcare provider, a health plan, or a healthcare clearing house). These activities involving the use or disclosure of PHI on behalf of a **covered entity** include, but are not limited to, claims processing, data collection and analysis, utilization review, and billing. Downstream vendors of a business associate may also be classified as business associates if they **create**, **receive**, **maintain,** or **transmit** PHI.

With increasing regulatory and contractual requirements for covered entities and business associates to establish and maintain safeguards over the use and disclosure of PHI, organizations are tasked to demonstrate their ability to manage the risks associated with **securing and guarding PHI**.


Receives
Transmits
Protected Health Information
Business associate
Business associates are organizations that create, receive, maintain, or transmit PHI.
Maintains
Creates

## Critical steps for every business associate

1. **Understand your regulatory and contractual requirements** for security and privacy protections, self-assessments, and third-party assurance.
2. **Determine the controls framework** and assurance programs that best meet your needs.
3. **Assess your current environment** and identify potential control gaps between your organization's current state and control framework requirements.
4. **Develop and execute a plan** to address identified gaps.
5. **Reassess current environment** postremediation.
6. **Execute an effective assurance program:** self-assessment and third-party

## Are you ready?

KPMG LLP's (KPMG) collective experience suggests that organizations are often overwhelmed with addressing and complying with the large number of regulatory and contractual requirements.

With little regulatory direction or guidance, business associates are faced with complex decisions on how to best meet their obligations to assess, design, and implement controls related to securing PHI. Faced with these complex decisions, business associates often turn to KPMG  for assistance in assessing their current state control environment against regulatory and contractual requirements. KPMG can help your organization by providing you with readiness assessments, remediation planning, and control design and implementation. Additionally, KPMG can provide your organization with attestation services including Service Organization Control® (SOC) reporting.

# How can KPMG help you?

**KPMG can provide a variety of services to assist business associates** in addressing their regulatory and contractual requirements.

## KPMG's Advisory Services

**Health Information Portability and Accountability Act (HIPAA) compliance assessments** – KPMG's HIPAA privacy and security risk assessments are designed to meet the regulatory requirements of the HIPAA Omnibus Rule and leverage our first-hand experience and deep regulatory insight to help organizations create and maintain sustainable HIPAA compliance programs. We understand what is required to conduct a robust risk assessment and have keen insight into why certain risk assessments fail to satisfy the standards set by the Office for Civil Rights (OCR).

**SOC 2® readiness assessments** – SOC 2® readiness assessments help organizations prepare for future SOC 2® attestation engagements by helping organizations understand the requirements of the standard, identify potential gaps between current state controls and the criteria for selected trust services principles, and provide observations and recommendations. SOC 2® + readiness assessments can also identify gaps against criteria from various frameworks as needed.

**HITRUST CSF readiness assessments** – Similar to a SOC 2® readiness, KPMG can assist you in understanding and completing a HITRUST CSF self-assessment on your way to HITRUST CSF certification.

## KPMG's Attestation Services

**SOC 2® –** *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, is an attestation examination performed by a service auditor to examine and report on controls at a service organization.

**SOC 2® + additional criteria** – A service organization may request that the service auditor's report address criteria in addition to the applicable trust services criteria. Additional criteria may be based on regulatory requirements, such as those established by HIPAA, or criteria established by an industry group, such as the Health Information Trust Alliance (HITRUST).

**HITRUST CSF certification testing** – A company, in rare cases, may only accept a HITRUST CSF Certification (HITRUST CSF validated assessment). KPMG can assist your organization in the process by performing testing necessary to submit to HITRUST for a HITRUST CSF validated assessment.

The great news is that if you are doing a SOC 2® and HITRUST validated assessment, KPMG can help you identify and realize efficiencies across your attestation portfolio by leveraging our strong knowledge of the frameworks and how they overlap.

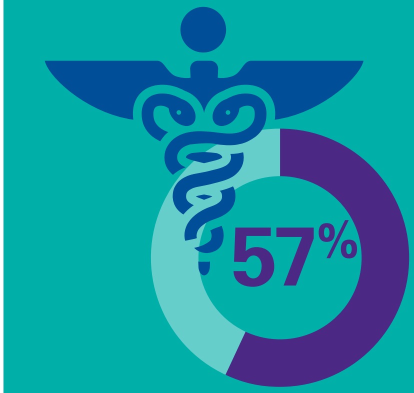
# Timing is everything

**Preparing to meet these security requirements is no easy task.** Doing it properly takes time and requires a methodical approach. Our experience suggests that it can take 18 to 36 months for an organization to adequately execute an effective self-assessment and third party assurance program. Given that most business associates will find themselves contractually obligated to provide some form of assessment or attestation within the next two years, it is clear that time is quickly running out.

# Did you know?

**In late 2015, HITRUST and the AICPA came together to align HITRUST's Common Security Framework with the AICPA's SOC 2® reporting.**

An expected outcome of the collaboration is to help organizations, such as business associates, comply with regulations and obligations and streamline SOC 2® reporting requirements.



**A KPMG survey found that 57% of health plans and providers see HIPAA violations as their top information security concern.**

Source: KPMG (2015). Health care and Cyber Security: IncreasingThreats Require Increased Capabilities

# Our clients choose KPMG because:

**We are the only firm to have worked with the OCR:** We developed and conducted their 2012 audits and defined the criteria to comply with the HIPAA regulation, providing us with an informed perspective on how the rules are applied.

**We understand security:** We have helped major healthcare organizations to understand their current state and gaps, develop recommendations to address their regulatory requirements, respond to breaches, and take corrective actions to resolve their security control issues.

**We have received recognition:** Forrester Research listed KPMG as the top firm in cybersecurity in 2016.

**We take a cross-functional approach:** We combine deep industry experience and market-leading security capabilities to help ensure our services are thorough, reliable, and practical.

**We are independent and objective:** As a recognized and trusted third-party adviser, we take an objective view of your environment to identify gaps and provide observations and recommendations.

**We lead the industry:** We are consistently recognized as an industry leader for security and leverage our position to conduct insightful research and bring key industry knowledge to our clients.

**KPMG, as a leading service provider, is ready to assist your organization in meeting the challenges and complex decisions evolving from the ever changing regulatory environment.**

**Whether facing explicit contractual requirements or not, many business associates are moving ahead with preparing their organizations for the rigors that come with these new and increasing requirements. Your organization can gain the confidence of your partners, meet customer demands, and create a competitive advantage by proactively demonstrating a serious commitment to information security.**

## Contact us

**Michael Ebert**
Partner, Healthcare Advisory
267-256-1686
mdebert@kpmg.com

**Emily Frolick**
Partner, Healthcare Advisory
513-763-2453
efrolick@kpmg.com

**Thomas Humbert**
Director, Healthcare Advisory
312-665-1593
thumbert@kpmg.com

**Matthew Sadler**
Director, Healthcare Advisory
717-260-4617
msadler@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

**kpmg.com/socialmedia**

**kpmg.com/app**

Download on the App Store