Deloitte.

Issue Brief:

Update: Privacy and security of protected health information

Omnibus Final Rule and stakeholder considerations

The transforming U.S. health care system is producing an immense volume of information, and much rides upon that information's availability, integrity, and confidentiality.

Implementing new care models, health insurance models, and structures/processes such as insurance exchanges, value-based payment systems, population health management, and personalized therapeutics requires meticulous management of vast quantities of personal information. This information is drawn from many disparate sources and delivered electronically to recipients including clinicians, insurers, and patients, generating attendant risk issues. In addition, mobile health, or mHealth, technologies and permeable boundaries among existing and new entrants in the health ecosystem increase the complexity of managing protected health information (PHI) and compound an already challenging issue for industry stakeholders (Figure 1).

How do privacy and security differ?

Privacy

- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (2003) states that information in any form – oral, paper, or electronic – that relates to a specific individual is protected health information, or PHI.[1,2] Under this rule, PHI may be shared with appropriate parties in the course of providing or receiving payment for health care. PHI also may be used to protect the public health and well-being, as in cases of research or legal proceedings.

Security

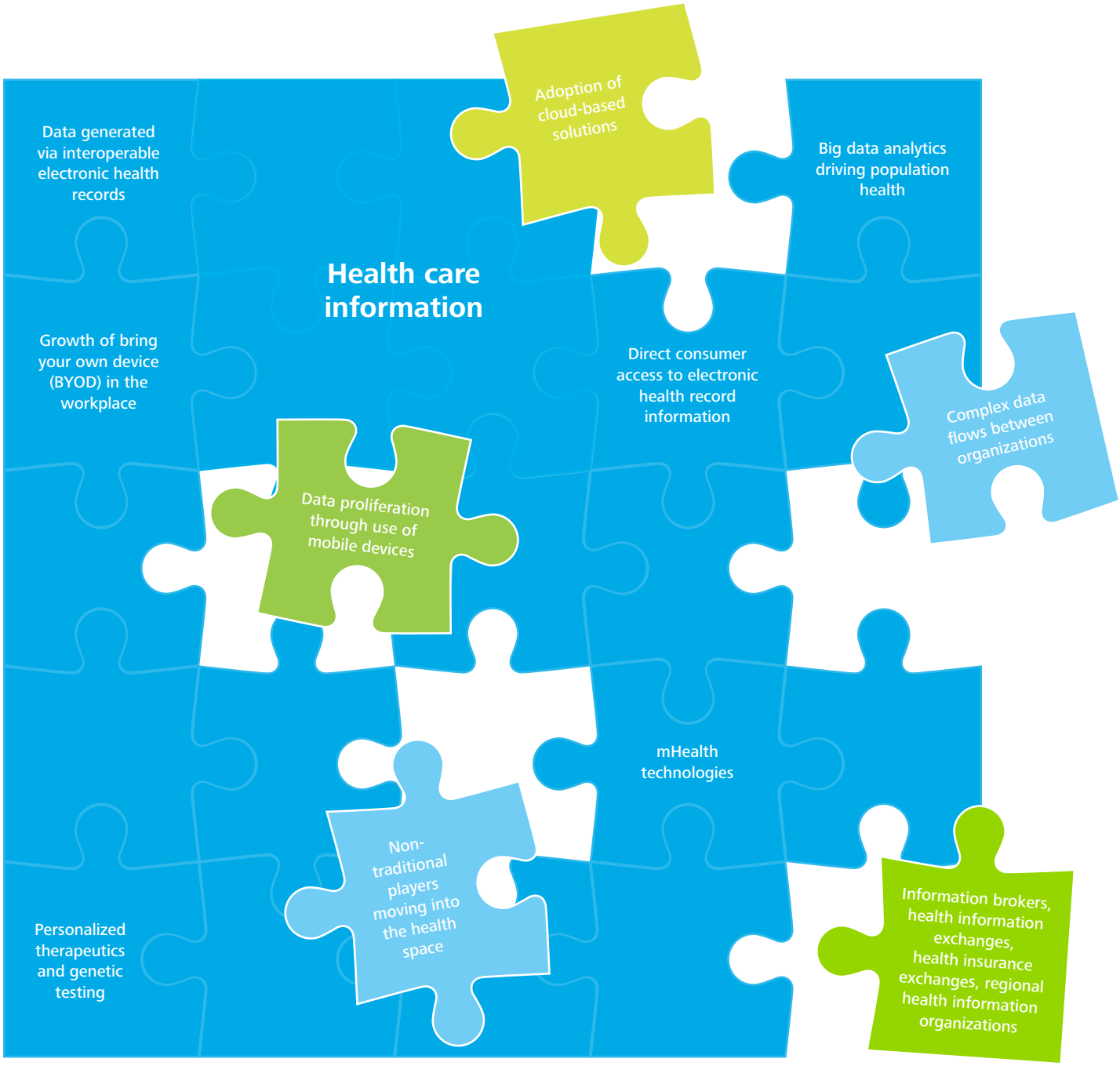
- The Security Rule of HIPAA (2003)[3,4] operationalizes the Privacy Rule. It requires that covered entities (defined as health plans, health care clearing houses, and health care providers who electronically transmit health care information connected with a transaction) ensure confidentiality, integrity and availability of all electronic PHI; that they anticipate information security threats, both intentional and unintentional; and that they ensure workforce compliance.
- With the HIPAA Omnibus Final Rule (2013), business associates (such as contractors or sub-contractors and defined as anyone who performs on behalf of a covered entity and is involved in the use or disclosure of individually identifiable health information such as claims processing, benefit administration, billing, data analysis, and so on) are now subject to these rules.

Produced by the Deloitte Center for Health Solutions

#ProtectedHealthInfo

Figure 1: Why is privacy and security of PHI an issue?

New and permeable boundaries are bringing many more players into contact with sensitive health information. Health care organizations are facing increasingly complex issues of data management and control, often with insufficient resources (human capital, financial, and technological) and expertise.



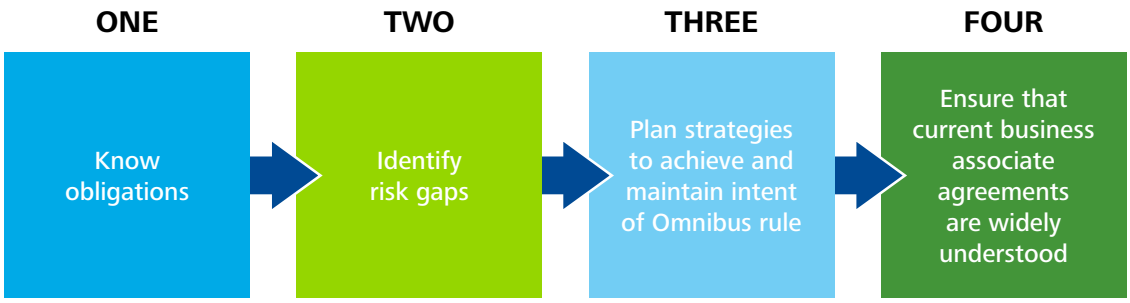
Health care transformation absent a trustworthy foundation is a risky venture. Sensitive personal information is vulnerable to employee error and negligence, as well as medical identity and financial identity theft. Safeguarding PHI is more important than ever.

In 2011, the Deloitte* Center for Health Solutions published the Issue Brief *Privacy and Security in Health Care: A Fresh Look*. This new Issue Brief discusses updates to privacy and security regulations, specifically the Omnibus Final Rule, as well as associated considerations for health care organizations.

The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule, effective March 26, 2013, greatly expands privacy and security standards, compliance actions, breach notification steps, and penalties. The new regulations allow for fines of more than $1 million for health record breaches. The permanent HIPAA audit program commences in 2014. The importance of ongoing risk analysis is a central feature of these audits.[5]

In September 2013, the Omnibus Final Rule became enforceable. Industry stakeholders should consider evaluating their HIPAA privacy and security controls as soon as possible (Figure 2).

Figure 2: Organizations should consider evaluating their HIPAA privacy and security controls



* As used in this document, "Deloitte" means Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

HIPAA Omnibus Final Rule

HHS issued the HIPAA Omnibus Final Rule in January 2013.[6] The rule's security and privacy implications lie in its strengthening of regulatory protections for patient information and increasing fines for HIPAA violations. The rule, in draft form since 2010, became enforceable September 23, 2013. Major changes include expanding individuals' rights to electronic copies of their medical records and expanding organizations subject to the Genetic Information Nondisclosure Act.

HIPAA Security and Privacy Audit Pilot Program

In December 2012, OCR completed a pilot program of HIPAA security and privacy audits.[7] A permanent HIPAA audit program begins in 2014.[8] Under the audit program, health care organizations can expect to be measured against all changes in the HIPAA Omnibus Final Rule, with special attention paid to risk analysis procedures and safeguards to prevent data breaches. No penalties were issued in the pilot program[9] but findings from the permanent program will be subject to the increased fines of the Final Rule.[10]

Background

In more than ten years following the April 2003 release of the HIPAA Final Rule, The Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) has investigated and resolved over 22,000 violations.[11] Since the September 2009 publication of the Breach Notification Rule, more than 800 large breaches (cases affecting more than 500 individuals each) involving the PHI of more than 29 million patients have been reported.[12] Issues found most frequently are impermissible uses and disclosures of protected health information, lack of safeguards of protected health information, and lack of patient access to their protected health information.[13] The most common cause of HIPAA violations has been lack of awareness of a given HIPAA requirement.[14] In addition, the OCR has concluded its pilot HIPAA audit program, and begins a full-scale audit program in 2014.[15]

HHS has taken a series of steps to strengthen patient privacy protections and to monitor and enforce these protections. The HIPAA Omnibus Final Rule strengthens regulatory protections for patient information, increases penalties for breaches, and emphasizes agreements with business associates. The OCR has conducted a pilot program of HIPAA Security and Privacy Audits, and is using its results to inform the full-scale security and privacy audit program beginning in 2014.[16]

Highlights of the HIPAA Omnibus Final Rule security and privacy provisions**

Among the key security and privacy provisions in the Omnibus Final Rule that warrant stakeholder attention are the following four items:

1. Liability for HIPAA violations increases substantially (Figure 3).

- Each individual HIPAA violation is now potentially subject to a fine of up to $50,000, increased from the earlier limit of $100.
- The yearly cap for violations of the same type is $1.5 million, up from $25,000.[17]

** Entities covered by the HIPAA Omnibus Final Rule are obligated to comply with all relevant requirements. Entities are encouraged to review the entire rule. Links to further resources can be found at the end of this brief.

2. Business associates (BAs) are now subject to HIPAA rules.

- In addition to covered entities, HIPAA now applies to business associates (companies that handle protected health information on behalf of covered entities).
- Previously, BAs were only required to contractually agree to handle PHI securely while conducting transactions. They were exempt from liability for penalties should a breach occur; covered entities had no enforcement rights. The new rule requires that covered entities have specific business agreements with each of their BAs and that BAs bear responsibility for their own data breaches.[18]
- In the Final Rule, HHS encourages covered entities to specify in the business agreement exactly how and when the BA will inform the covered entity of the breach.[19]

3. All health plans are prohibited from using genetic information for underwriting purposes.

- The Genetic Information Nondisclosure Act (2008) (GINA) originally prohibited four types of health plans from using an individual's genetic information for underwriting purposes, including group health plans, health insurance issuers, HMOs, and supplemental Medicare plans.
- The Omnibus Final Rule expands this prohibition to all health plans.[20]
- To comply with this rule, health plans will need to implement procedures that clearly limit access of their underwriting functions to patients' genetic information received as part of the claims process.

Further proposed rules underscore seriousness of privacy and security

HHS continues to refine and formulate its security and privacy guidelines. In January 2014 HHS published a proposed rule that would require health plans to certify the security of certain electronic transactions with a third party. Fines for failing to do so would be significant: one dollar per covered life per day of noncompliance, up to $20 per covered life. Knowingly providing inaccurate or incomplete information would result in fines of $40 per covered life. This proposed rule further illustrates how serious regulators are about information security in health care, and how consequences have grown proportionally.[24,25]

4. Both covered entities and BAs are now required to provide individuals with electronic copies of their medical records upon request.[21]

- The format of the electronic copy may be agreed upon by the individual and the covered entity.[22]
- The new rule shortens the time limit for delivering the electronic copies from a maximum of 90 to 30 days. Some allowances are made for a single 30-day extension.[23]

Figure 3: HIPAA violation liability

Tier of violation	Each violation	All such violations of identical provision in calendar year
	2013	
Without knowledge or intent	$100-$50,000	$1,500,000
Due to reasonable cause	$1,000-50,000	$1,500,000
Willful neglect – corrected	$10,000-50,000	$1,500,000
Willful neglect – not corrected	$50,000	$1,500,000

Source: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Federal Register 17, 5583

Emerging issue: Medical device security

Medical device security is a growing concern. Recent demonstrations have shown that in some devices settings can be changed remotely and malware uploaded. In addition, devices can be subject to a denial-of-service attack.[26]

- **Risk of patient harm.** Unauthorized remote access could change a device's settings or cause it to stop working completely.[27]
- **Risk of widespread PHI vulnerability.** Health IT networks are at risk through connected medical devices. As some devices can be accessed remotely, hackers may potentially access health IT networks via these devices.[28]
- **Regulations still in development.** The FDA has released guidelines on cyber security for medical devices and hospital networks that identify cyber-security issues manufacturers should consider when preparing market submissions for medical devices in order to maintain information confidentiality, integrity, and availability.[29]

HIPAA Security and Privacy Audit Pilot: Few health care organizations have appropriate controls in place

The HIPAA audit program was the first security and privacy audit program by a regulatory body in the health care industry.[30] The program was intended to assess HIPAA compliance across covered entities, identify best practices, and identify vulnerabilities. Preliminary results show a large gap between regulatory requirements and the industry's preparation to meet them.

- The pilot audits were conducted in 2011 and 2012 on 115 covered entities, spanning health plans, health care providers, and health care clearing houses. Most audits resulted in negative findings,[31,32] indicating that the industry needs to improve its security and privacy programs significantly before the permanent audit program begins.
  - Only 13 organizations, or 11 percent of all participants, passed the audit without any issues.[33]
  - 60 percent of audited organizations had not performed a complete and accurate risk assessment.[34]
  - 30 percent of the audits' 980 negative findings were due to lack of awareness of HIPAA security and privacy requirements.[35]

Security and privacy practices in the health care industry need to change

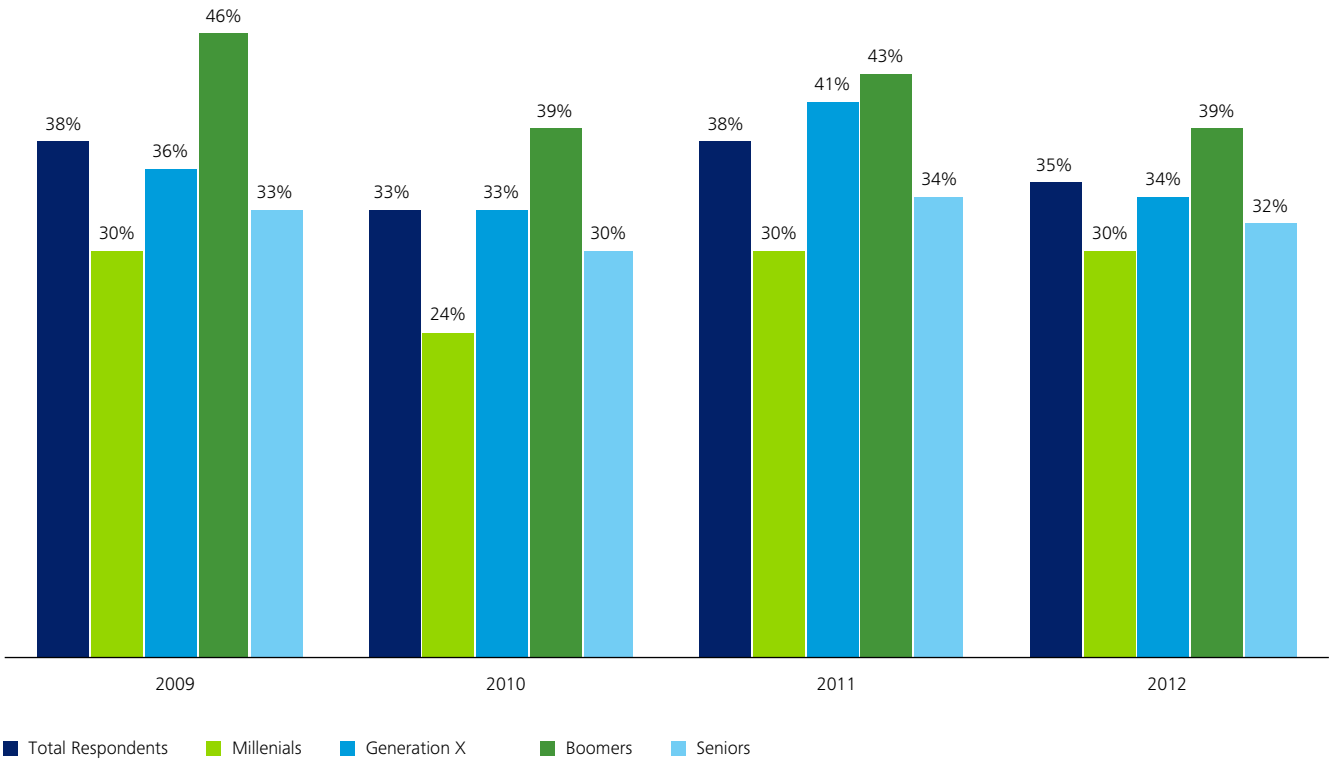
Potential economic and reputational damage may arise if organizations lack appropriate HIPAA security and privacy controls:

- **Financial penalties**
  - In 2013, OCR issued resolution agreements for violations that included settlements between $50,000 and $1.7 million.[36]
  - These cases involved improper safeguarding of records for anywhere from one to more than 600,000 patients.
- **Lost productivity and other costs**
  - The total annual cost of dealing with data breaches to the health care provider sector alone is estimated at $7 billion.[37]
  - The average per-record cost of a data breach for a health care organization in 2013 is $305.[38]
  - The average cost to a health care organization of dealing with data breaches (over the two-year period of 2010-2011) is estimated at $2.4 million.[39]
  - Failure to comply with the new HIPAA guidance may result in missed financial opportunities through bonuses (e.g., meaningful use bonus payments) and lost patient volumes.
- **Brand and reputational loss**
  - More than 180 large breaches involving more than 6.9 million records were reported in 2013.[40]
  - HIPAA Act breaches are made publicly available on the HHS website in a searchable and analyzable database, "Data Breaches Affecting 500 or More Individuals." It is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.
- **Loss of consumer goodwill**
  - Consumers' concerns about the security of their personal information, and greater transparency of performance information, may lead consumers to avoid organizations with a history of breaches. For example, one study reported that 60 percent of patients who were victims of a privacy breach no longer seek care from that provider.[41]
  - In 2012, the average lifetime value of one lost patient was estimated at $111,000, up 3.9 percent from 2010.[42]

Deloitte Survey of U.S. Health Care Consumers: Privacy and security concerns

- Even as threats to the safety and privacy of medical information increase, consumers' concerns about potential risk have remained constant over the past four years: Around 35 percent of consumers are strongly concerned about risk. (See figure below).
- Concern varies by generational group, with those ages 18-30 being more relaxed about security threats to personal information occurring via Internet transmission.

How concerned are you that the privacy and security of your personal health/medical information might be at risk …if you share information with your doctor through an Internet connection?



Those reporting 8, 9 or 10 on a 10-point scale where 10 is 'extremely concerned'

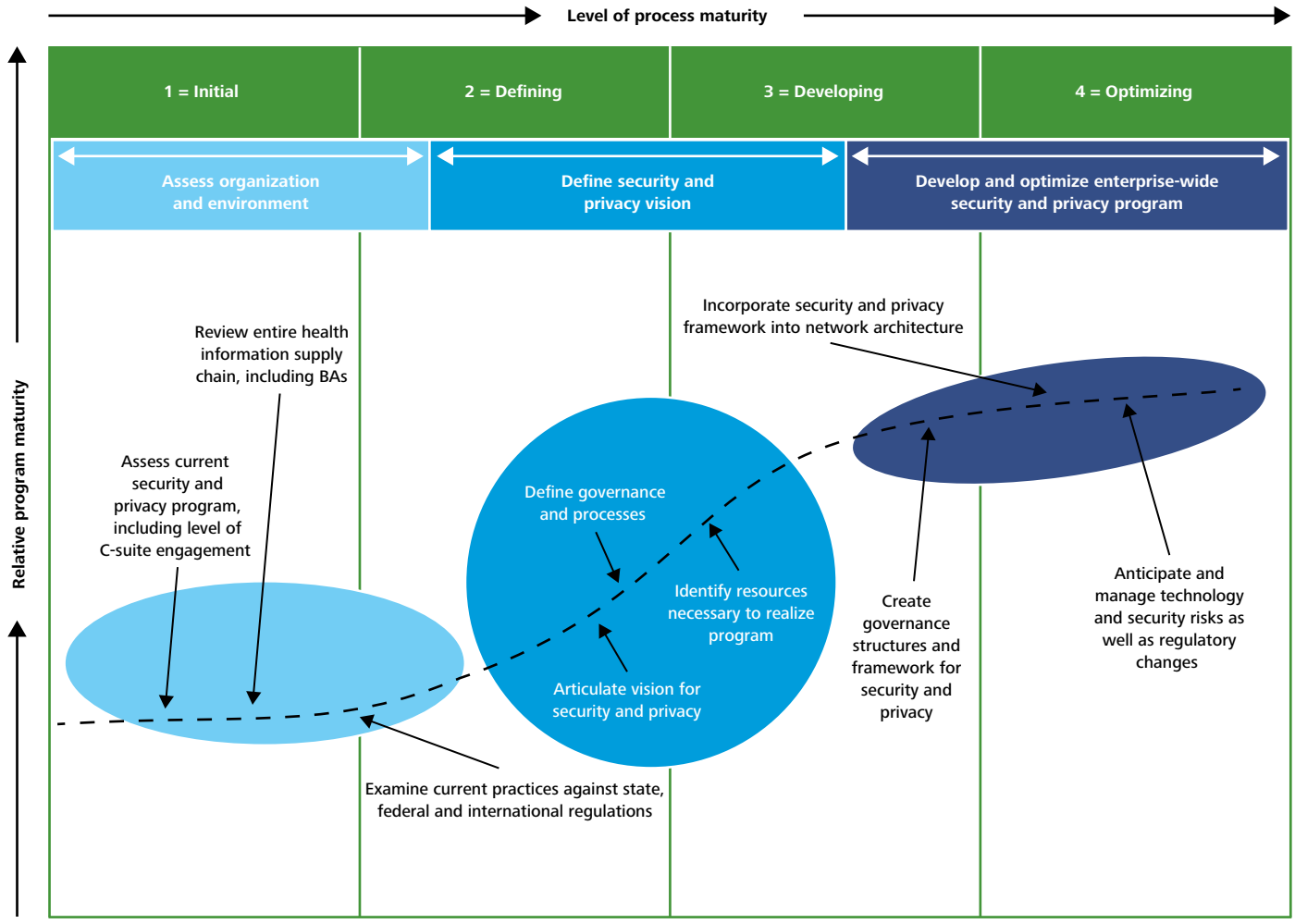
Deloitte Survey of U.S. Health Care Consumers, 2009-2012

Stakeholder considerations

With the Omnibus Final Rule in place and potential HIPAA audits on the horizon, industry stakeholders – providers, health plans, retail health, bio-pharma, and medical device companies – should consider whether they have a need to promptly **assess** potential capability gaps, **define** their security and privacy vision and needs, and **develop** appropriate remediation programs (Figure 4). One such approach is discussed below.

These steps are integral to the process of becoming secure, vigilant, and resilient in the face of threats to information security.

Figure 4: Security and privacy maturity model



1. Assess: Organization and environment

- Perform a risk review of the full health information supply chain, covering internal operations as well as outside business associates and subcontractors. The review could cover:
  - Current technologies, applications, networks
  - Processes, policies, governance, PHI access
  - Locations, partners, third parties
  - State, federal, and international (cross-border) regulations and requirements

2. Define: Security and privacy vision and needs

- Articulate the organizational vision for security and privacy, and capture policies and processes in an organization-wide plan that also includes business associates. Based on the current state and external environment, this plan could:
  - Identify organizational gaps
  - Outline the organizational vision for security and privacy
  - Define governance and processes

3. Develop: An enterprise-wide privacy and security program

- If needed, invest in and implement a security and privacy program that includes continuous monitoring and updating. This could:
  - Create organizational governance structures for oversight of security and privacy
  - Incorporate a framework for a security and privacy management architecture
  - Articulate security and privacy policies and standards
  - Proactively define and manage the most critical technological and network risks
  - Develop identity and access controls and monitoring protocols

As the electronic transmission of PHI among U.S. health care system stakeholders proliferates, safeguarding the security and privacy of that information will become an increasing challenge. Organizations seeking to stay ahead of the regulatory curve should prepare now to address the near- and long-term implications of the Omnibus Final Rule.

Integration of these insights is one of the first steps for health care organizations towards becoming a secure, vigilant and resilient organization that values and protects its patients' PHI.

Useful resources

- Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (January 25, 2013) http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- The Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (2008) http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf
- American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), Division A, Title XIII and Division B, Title IV, Health Information Technology for Economic and Clinical Health Act (HITECH Act) (codified at 42 U.S.C. § 17930, et seq). http://www.gpo.gov/fdsys/pkg/USCODE-2011-title42/pdf/USCODE-2011-title42-chap156-subchapIII-partA.pdf
- U.S. General Accounting Office, Medical Devices: FDA Should Expand its Consideration of Information Security For Certain Types of Devices, August 2012. http://www.gao.gov/assets/650/647766.pdf
- Deloitte Center for Health Solutions, Issue Brief: Privacy and Security in Health Care: A fresh look, February 2011. http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/Health%20Reform%20Issues%20Briefs/US_CHS_PrivacyandSecurityinHealthCare_022111.pdf

To begin a discussion or for further information on security and privacy in the Life Sciences and Health Care industry, please contact:

Mark Ford
Principal
Cyber Risk Services
Life Sciences and Health Care
Deloitte & Touche LLP
mford@deloitte.com

Russ Rudish
Principal
AERS Life Sciences and Health Care Leader
Deloitte & Touche LLP
rrudish@deloitte.com

Peter Micca
Partner
National AERS Sector Leader – Health Plans
Deloitte & Touche LLP
pmicca@deloitte.com

Jennifer Malatesta
Principal
Life Sciences Advisory Services Leader
Deloitte & Touche LLP
jemalatesta@deloitte.com

Steve Burrill
Partner
Advisory Health Care Provider Leader
Health Care Providers Marketplace Leader
Deloitte & Touche LLP
sburrill@deloitte.com

Authors

Sheryl Coughlin, PhD, MHA
Head of Research
Deloitte Center for Health Solutions
Deloitte Services LP
scoughlin@deloitte.com

Ryan Carter
Senior Market Research Analyst
Deloitte Services LP
rycarter@deloitte.com

Acknowledgements

We would like to thank Harry Greenspun MD, Technical Adviser, Center for Health Solutions, as well as Larisa Layug, Wendy Gerhardt of Deloitte Services LP, and the many others who contributed to this report.

Contact information

To learn more about the Deloitte Center for Health Solutions, its projects and events, please visit www.deloitte.com/centerforhealthsolutions.

Deloitte Center for Health Solutions
1001 G Street N.W.
Suite 1200
Washington, DC 20001
Phone 202-220-2177
Fax 202-220-2178
Toll free 888-233-6169
Email healthsolutions@deloitte.com
Web www.deloitte.com/centerforhealthsolutions

Follow @DeloitteHealth on Twitter

#ProtectedHealthInfo

To download a copy of this brief, please visit www.deloitte.com/us/protectedhealthinfo.

References

1 HHS OCR, Summary of the HIPAA Privacy Rule, May 13 2003, via http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

2 The HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and Eof Part 164, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

3 HHS, Summary of the HIPAA Security Rule, accessed via http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.htm

4 The HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164

5 Health IT Security, OCR director Leon Rodriguez previews HIPAA audit strategies, September 23, 2013, via http://healthitsecurity.com/2013/09/23/ocr-director-leon-rodriguez-previews-hipaa-audit-strategies/

6 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (January 25, 2013) via http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

7 HHS OCR, HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis, HCCA 2013 Compliance Institute, April 23 2013, http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf

8 Healthcare Info Security, What's ahead for HIPAA Audits, April 2 2013, http://www.healthcareinfosecurity.com/whats-ahead-for-hipaa-audits-a-5647/op-1

9 HHS OCR, HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis, HCCA 2013 Compliance Institute, April 23 2013, http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf

10 Health Data Management. What HHS/OCR will look for in HIPAA compliance audits, Mar 21, 2013, via Factiva.

11 Department of Health and Human Services (HHS) Office of Civil Rights (OCR), Health Information Privacy Enforcement Highlights, December 31 2013. Accessed January 22 2014 via http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html

12 Department of Health and Human Services (HHS) Office of Civil Rights (OCR), Breaches affecting more than 500 individuals. Accessed January 22 2014 via http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

13 Department of Health and Human Services (HHS) Office of Civil Rights (OCR), Health Information Privacy Enforcement Highlights, December 31 2013. Accessed January 22 2014 via http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html

14 HS OCR, HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis, HCCA 2013 Compliance Institute, April 23 2013, via http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf

15 Health Data Management. What HHS/OCR will look for in HIPAA compliance audits, Mar 21, 2013, via Factiva.

16 Health Data Management. What HHS/OCR will look for in HIPAA compliance audits, Mar 21 2013, via Factiva.

17 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule. 78 Federal Register 17, January 25 2013, 5583, via http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

18 Ibid., 5589

19 Ibid., 5656

20 Ibid., 5659

21 Ibid., 5633

22 Ibid., 5632

23 Ibid., 5637

24 Mondaq, HHS issues proposed rule requiring health plans to demonstrate compliance with HIPAA electronic transaction standards and operating rules, January 9, 2014. Via Factiva

25 Federal Register, Vol. 77 no. 1, Thursday Jan 2, 2014, Rules and Regulations @ 298, via https://www.federalregister.gov/articles/2014/01/02/2013-31318/administrative-simplification-certification-of-compliance-for-health-plans

26 U.S. General Accounting Office, Medical Devices: FDA Should Expand its Consideration of Information Security For Certain Types of Devices, August 2012, p15-16, via http://www.gao.gov/assets/650/647766.pdf

27 U.S. General Accounting Office, Medical Devices: FDA Should Expand its Consideration of Information Security For Certain Types of Devices, August 2012, p15-16, via http://www.gao.gov/assets/650/647766.pdf

28 Department of Homeland Security, National Cybersecurity and Communications Integration Center, Attack Surface: Healthcare and Public Health Sector, May 15 2012. Accessed May 5 2013 via http://publicintelligence.net/nccic-medical-device-cyberattacks/

29 FDA, FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks, June 13, 2013, via http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm?source=govdelivery

30 Subject Matter Expert interview with Mark Ford, March 29 2013.

31 HHS OCR, HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis, HCCA 2013 Compliance Institute, April 23 2013, via http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf

32 Modern Healthcare, Audits find organizations unaware of new data, privacy rules, April 23 2013, via http://www.modernhealthcare.com/article/20130423/NEWS/304239958

33 HHS OCR, HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis, HCCA 2013 Compliance Institute, April 23 2013, via http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf

34 HHS OCR, HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis, HCCA 2013 Compliance Institute, April 23 2013, via http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf

35 HHS OCR, HIPAA Privacy, Security and Breach Notification Audits Program Overview & Initial Analysis, HCCA 2013 Compliance Institute, April 23 2013, via http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf

36 Lexology, Healthcare Privacy—2013 year in review, January 2, 2014. Accessed January 22, 2014 via http://www.lexology.com/library/detail.aspx?g=fe0a8747-de56-4fd5-9ec7-51eeeb20f8fa

37 Ponemon Institute, Third Annual Benchmark Study on Patient Privacy and Data Security, December 2012. http://www2.idexpertscorp.com/ponemon2012/

38 Ponemon Institute, 2013 Cost of Data Breach Study: United States, May 2013. Accessed June 7, 2013, via http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf

39 Ponemon Institute, Third Annual Study on Patient Privacy, November 2012. Accessed February 27, 2013, via http://www2.idexpertscorp.com/ponemon2012/

40 Department of Health and Human Services (HHS) Office of Civil Rights (OCR), Breaches affecting more than 500 individuals. Accessed January 22 2014 via http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

41 FairWarning, How privacy considerations drive patient decisions and impact patient care outcomes, September 2011. Accessed June 7, 2013, via http://www.fairwarning.com/whitepapers/2011-09-WP-US-PATIENT-SURVEY.pdf

42 Ponemon Institute, Third Annual Benchmark Study on Patient Privacy and Data Security, December 2012. http://www2.idexpertscorp.com/ponemon2012/

Deloitte Center for Health Solutions

About the Deloitte Center for Health Solutions
The Deloitte Center for Health Solutions is the health services research arm of Deloitte LLP. Our goal is to inform all stakeholders in the health care system about emerging trends, challenges, and opportunities using rigorous research. Through our research, roundtables, and other forms of engagement, we seek to be a trusted source for relevant, timely, and reliable insights.