PUBLIC HEALTH INSTITUTE®

Comparing Breaches of Unsecured Protected Health Information Among Business Associates and Covered Entities in California and the United States

FEBRUARY 2017

Contents

Author

Theodore (Theo) Tsoukalas, Ph.D., Public Health Institute, Oakland, CA

About the Public Health Institute

The Public Health Institute (PHI) is dedicated to promoting health, well-being and quality of life for people throughout California, across the nation and around the world. Visit www.phi.org to learn more.

Acknowledgments

The author would like to thank Claudia Page, an independent health care consultant working with CHCF on HIPAA and data privacy related projects, for her guidance and support throughout the project. The author also wishes to thank CHCF* for its fiscal sponsorship and PHI for its administrative support.

*Supported by the California Health Care Foundation, which works to ensure that people have access to the care they need, when they need it, at a price they can afford. Visit www.chcf.org to learn more.

Introduction

More and more healthcare providers and insurers are contracting out aspects of healthcare administration, such as lab work and imaging, billing, and records management, to third parties. Known as Business Associates (BAs), these organizations and companies are independent from traditional Covered Entities (CEs), such as hospitals and health insurers. Because BAs are not exempt from data breaches, and in fact are vulnerable to them, there is an urgent need to understand the causes and impacts of breaches among BAs and to compare them to those of CEs.

This report examines this phenomenon nationally and in California over a six-year period to better understand the vulnerabilities and who is impacted, to help inform policy, and to improve consumer protection from data breaches of unsecured protected health information.

Legislative Context

The privacy and security of confidential medical information is protected by federal and California legislation. The federal Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) protect the privacy and security, respectively, of patient health information (PHI). HIPAA has been protecting the privacy of patient health data since 2000. Since 2009, the year HITECH went into effect, the electronic storage, transmission, and sharing of patient health data have been protected in the context of health information technology and electronic health records. HITECH directs the secretary of Health & Human Services (HHS) to report breaches of unsecured protected health information affecting 500 or more individuals.

In California, the first state in the US to enact privacy protection of information gathered, stored, transmitted, and managed using electronic technologies, the legislative and regulatory basis for such protection is rooted in two pieces of legislation enacted in 2002—AB 700 (Simitian) and SB 1386 (Peace). Data of such breaches have been collected by the HHS secretary since the last quarter of 2009, and a single breach can range from impacting 500 individuals to millions of individuals in any given year across the United States. Specifically, for the data years 2010-2015 the number of impacted individuals ranged from 500 to 78.8 million—such as Anthem Indiana's breach reported by the HHS secretary in March 2015. Every year, the protection of patient health information is compromised from breaches that occur due to hacking, theft, loss of paper records, misdirection of communications, unauthorized access, and other causes. Ransomware attacks fall under the Hacking/IT Incident breach category.

HIPAA and HITECH direct Covered Entities (CEs) and Business Associates (BAs) of CEs to put in place administrative and technology-based safeguards and standards to secure protected health information.

In addition, the 2013 Omnibus Rule, which implemented changes to HIPAA and HITECH, expanded the definition of BA to include subcontractors who create, receive, maintain, or transmit PHI on behalf of another BA.

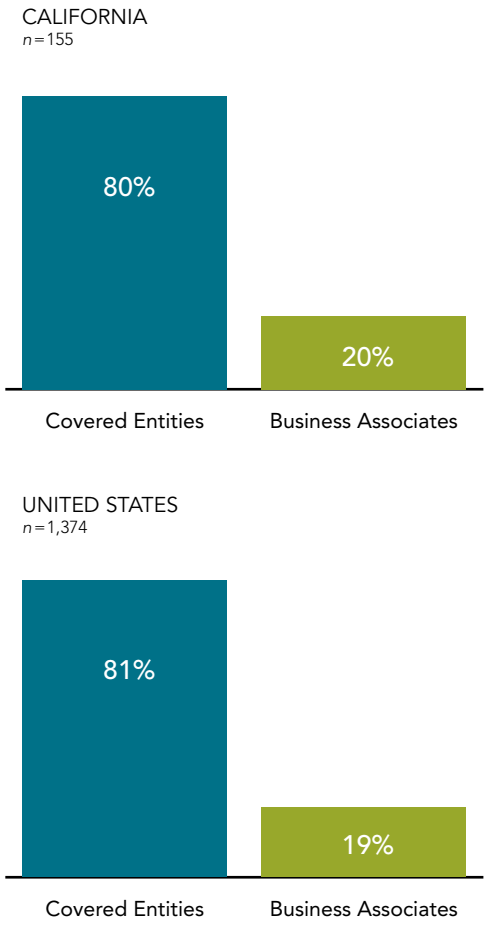
(See Appendix A: California and US Data Breach Legislative Highlights for more details.)

Findings: A Comparative Analysis of Breaches in California and the US

At the national level, a comparison between Covered Entities and Business Associates revealed that eight out of ten breaches originated from Covered Entities, and the rest from Business Associates.

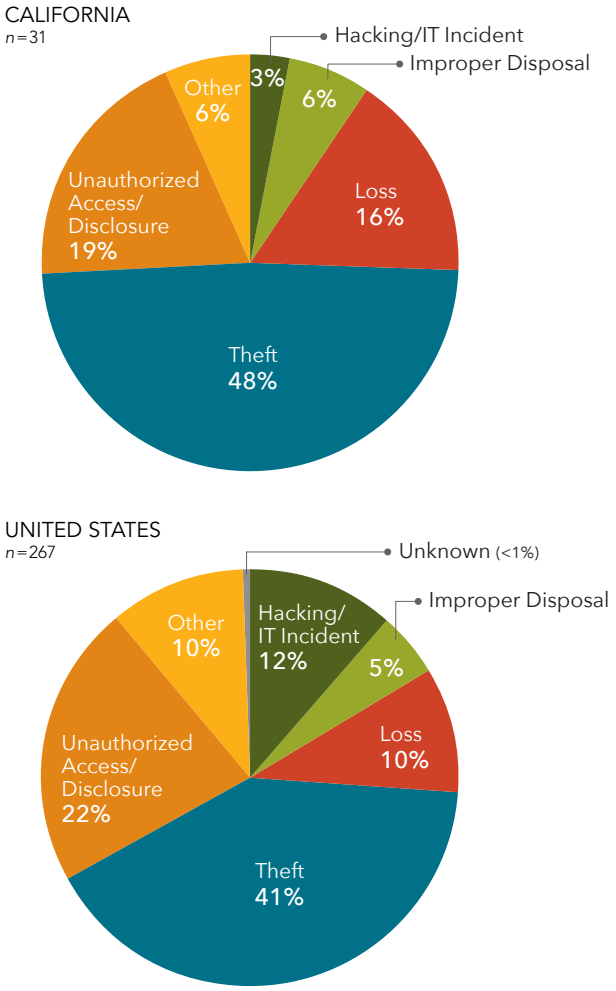
Occurrence of breaches for CEs and BAs. The percentage of breaches reported by California's CEs (80.00%) and BAs (20.00%) is similar to breaches among the US's CEs (80.57%) and BAs (19.43%) (Figure 1).

FIGURE 1. Breaches of Unsecured PHI Affecting 500+ Individuals, CEs vs. BAs, CA and US, 2010-2015



Causes of breaches for BAs. California's BAs reported a higher percentage of breaches caused by theft (48.39%) than BAs at the national level (40.82%). Other causes of breach among California BAs that are higher than the national average include Loss (16.13%) and Improper Disposal (6.45%) (Figure 2).

FIGURE 2. Causes of Breaches of Unsecured PHI Affecting 500+ Individuals, BAs, CA and US, 2010-2015

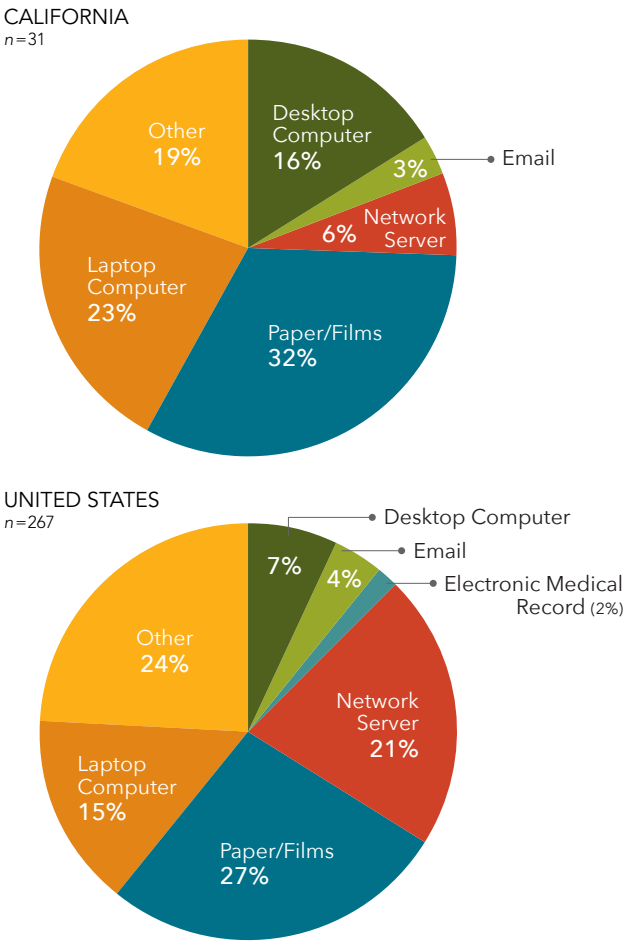


Note: Segments may not add to 100% due to rounding.

Sources of breaches for BAs. California BAs reported higher percentages of sources of breach than the United States average in Paper/Films (32.26%), Laptop Computers (22.58%), and Desktop Computers (16.13%) (Figure 3, page 5).

Data Source (Figures 1 and 2): US Dept. of Health & Human Services, Office of Civil Rights, Breaches Affecting 500 or More Individuals.

FIGURE 3. Sources of Breaches of Unsecured PHI Affecting 500+ Individuals, BAs, CA and US, 2010-2015



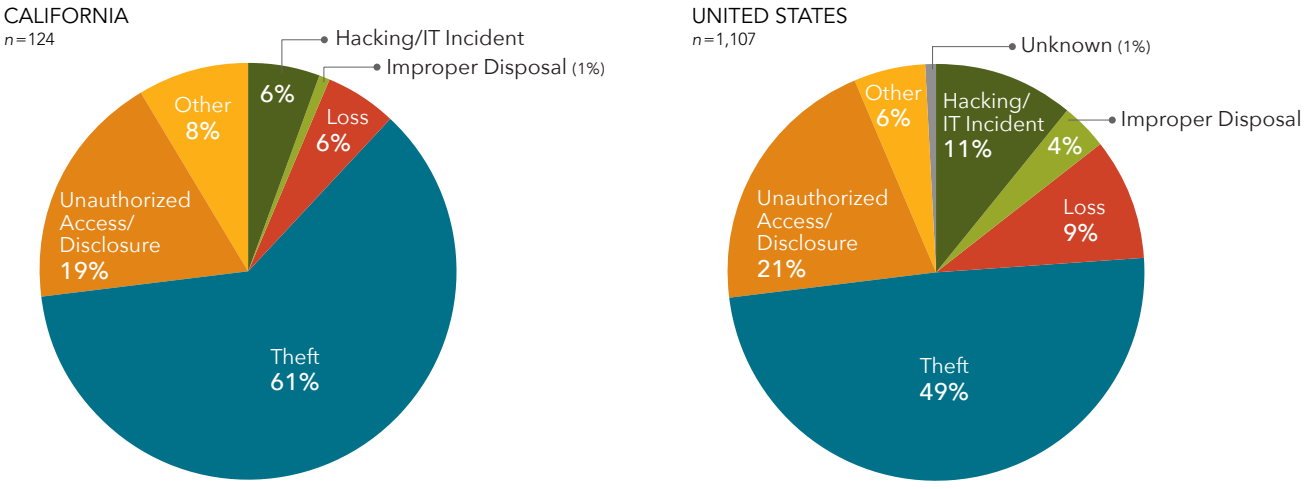
Impact of breaches on individuals. At the national level, a comparison between Covered Entities and Business Associates revealed the following:

- Health Plan breaches account by far for the largest percentage of individuals affected (70.55%) during the 2010-2015 data period.
- Breaches reported by Healthcare Providers (a subcategory of Covered Entities experiencing 68.78% of all breaches) affected 13.15% of the total number of individuals affected by all breaches.
- Business Associate breaches (with 19.43% of all breaches) affected a higher percentage of individuals (16.29%) than those affected by Healthcare Providers during the 2010-2015 data period. See Table 7 in Appendix B for more details.

In California, the same comparison produced a different finding: California breaches reported by Healthcare Providers (a subcategory of Covered Entities) impacted nearly all individuals (97.25%) affected by breaches reported by both Covered Entities and Business Associates. See Table 8 in Appendix B for more details.

Causes of breaches for CEs. California CEs reported a higher percentage of breaches caused by Theft (61.29%) than CEs at the national level (49.14%). Other causes (e.g., Postal Mail) of breaches (8.06%) among California CEs were also higher than the national average of 5.51% (Figure 4).

FIGURE 4. Causes of Breaches of Unsecured PHI Affecting 500+ Individuals, CEs, CA and US, 2010-2015

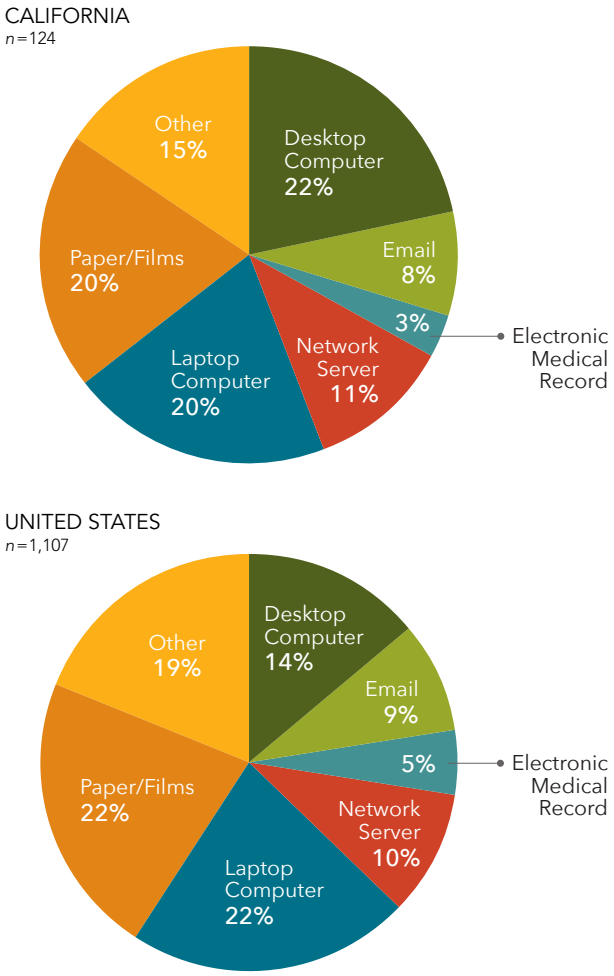


Note (Figures 3 and 4): Segments may not add to 100% due to rounding.

Data Source (Figures 3 and 4): US Dept. of Health & Human Services, Office of Civil Rights, Breaches Affecting 500 or More Individuals.

Sources of breaches for CEs. California CEs reported a higher percentage of Desktop Computers (21.77%) and Network Servers (11.29%) as sources of breach than the national average (13.91% and 9.76%, respectively). See Figure 5 for more details.

FIGURE 5. Sources of Breaches of Unsecured PHI Affecting 500+ Individuals, CEs, CA and US, 2010-2015



Note: Segments may not add to 100% due to rounding.

Data Source: US Dept. of Health & Human Services, Office of Civil Rights, Breaches Affecting 500 or More Individuals.

As the findings above suggest, California CEs and BAs reported higher percentages of theft than the national average. Based on these findings, the investigation performed an in-depth analysis of Web Descriptions accompanying theft reports to determine what was stolen, in what quantities, from what types of physical locations, and what numbers of individuals were affected. See Appendix B for details.

Conclusions

This investigation recognizes that, in part because the HHS database on breaches of unsecured protected health information affecting 500 or more individuals is constantly updated, additional research is required on such breaches, especially those impacting California. Nevertheless, a number of policy-relevant findings and trends have emerged from the analysis conducted thus far. Detailed conclusions of this study are located in Appendix C.

Business Associates are more vulnerable than CEs—in CA and US.

- Among US Covered Entities and Business Associates, breaches reported from Business Associates have affected a larger percentage of the total number of individuals affected than Healthcare Providers (13% among Healthcare Providers versus 16% among Business Associates—see Table 7 in Appendix B).
- This finding echoes the comments of HHS Secretary Kathleen Sebelius, who upon announcing HHS's HIPAA Omnibus Rule of 2013, observed that some of the largest breaches in the US have come from Business Associates.

Theft is a major area of vulnerability.

- Theft as a cause of breaches among California's Covered Entities and Business Associates is higher (by 12 percentage points for CA Covered Entities and by 8 percentage points for CA Business Associates) than that of their respective counterparts at the national level.
- Theft (all theft) makes the largest category of breaches in the United States and in California.

California CEs have higher rates of desktop computer and network server theft than the rest of the US.

- As revealed by the Web Descriptions analysis, California CEs have higher rates of desktop computer and network server theft than the rest of US.
- In addition, the overall theft of electronic devices among California's Covered Entities has pointed to several trends:
  - Overall theft among California Covered Entities has impacted more than twice as many individuals than the national average.

- Thefts of laptop computers reported by California Covered Entities have impacted more than twice as many individuals than the national average for the 2010-2015 reporting years.
- Thefts of network servers reported by California Covered Entities has impacted individuals at a rate nearly three times higher than the national average, and theft of desktop computers has impacted 1.5 times more individuals than the national average.

California BAs have higher rates of desktop computer and portable electronic storage device theft than the rest of the US.

- The analysis of text from Web Descriptions has revealed a number of policy-relevant findings and trends:
  - California Business Associates experienced a rate of desktop computer theft that was 8.26 times higher than the national average.
  - California Business Associates experienced a theft rate of portable electronic storage devices that was two times higher than that of the US average.
  - Overall, California Business Associates experienced a rate of theft for all types of devices 2.69 times higher than the national average.
- More importantly, however, the analysis of Web Descriptions points to a disturbing finding: The rate of thefts of desktop computers reported by California Business Associates have impacted 8.21 times more individuals than the national average for the 2010-2015 reporting years.

California BA offices are more vulnerable to theft than the rest of the US.

- California's Business Associate offices, as a type of physical location in which theft of electronic devices occurred, had a standardized rate two times higher than the US.
- The rate of individuals affected by Business Associate thefts of electronic devices occurring in offices is over six times higher (6.39 times) for California Business Associates than the US average.

Next Steps

Protected health information privacy and security stakeholders in California need to be aware that they have higher rates of theft than the rest of the nation.

- Business Associates need to be aware that they have a much higher rate of theft of desktop computers than the rest of the nation, which in turn impacts a very high rate of individuals compared to the rest of the nation—BA offices and vehicles have rates of physical locations of theft twice that of the rest of the nation.
- Policymakers and state officials who oversee the protection of health information data should continue to analyze breach data to inform evolving regulatory and policy activities.
- Federal agencies such as the Office of the National Coordinator and the Office for Civil Rights might consider a combination of stricter enforcement practices and education/training to encourage CEs and BAs to substantially minimize the conditions under which thefts of electronic devices occur.
- Finally, both federal agencies and CEs and BAs need to work together to create a sustainable model that would lead to encryption for all devices, including portable electronic storage devices, through a registration and certification process.

Methodology

Using a database of breaches (2010-2015) of unsecured protected health information (PHI) from the US Department of Health & Human Services (HHS), this investigation focuses on comparing data from California CEs and BAs with national data in two areas: (1) overall breaches of unsecured protected PHI and (2) an in-depth comparison of breaches of unsecured PHI caused by theft of electronic devices. The deeper focus on theft is prompted by findings from an earlier phase of this investigation suggesting that California CEs and BAs were reporting higher percentages of breaches caused by theft than the national average. To better understand this phenomenon, the researchers conducted an in-depth analysis of text available in certain descriptions in the Web Description section of the HHS database for data years 2010-2015 describing details of thefts (Type of Breach) to determine the type and number of electronic devices stolen, the type and number of physical locations involved, the work roles of people from whom the devices were stolen, and the number of individuals affected. United States and California Covered Entities and Business Associates were analyzed using standardized comparisons per 100,000 population (US Census Bureau 2015 population estimates). (See Appendix B for additional methodology considerations.)

See Appendices A and B for reference sources.

Appendix A. California and US Data Breach Legislative Highlights

California

In 2002, California became the first state in the nation to enact data breach notification legislation via SB 1386 and AB 700. The law resulting from SB 1386 and AB 700 "require[d] a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" (effective July 1, 2003).[1]

From 2003 to 2016, California legislation refined the definition of protected personal information by adding new elements to it:

- AB 1950 was codified in Cal Civil Code § 1798.81.5 and required businesses to have in place security procedures to protect personal information (effective January 1, 2005).[2,3]
- AB 1298 added medical information and health insurance information to the list of protected personal information (effective January 1, 2008).[4]
- SB 24 added to the protected personal information breach notice new requirements and required state and local government agencies and private businesses to supply the California attorney general with an electronic copy of the security breach notification for breaches affecting 500 or more individuals (effective January 1, 2012).[5]
- SB 46 added a person's online account credentials (i.e., user name, email address, password, or security question or answer) to the list of items considered protected personal information. A state agency or private business data breach involving any of the items that constitute "personal information," including items that resulted from the enactment of SB 46, would now trigger a breach notice event (effective January 1, 2014).[6]
- AB 1710 introduced three new requirements:
  - Entities of data breaches of personal information that included Social Security numbers and driver's license numbers are required to supply victims with at least one year of identity theft prevention services.
  - Entities that maintain personal information about Californians are required to install and maintain appropriate security measures to protect personal information.
  - Subcontractors (via contract from entity) are required to also install and maintain reasonable security procedures to protect personal information (effective January 1, 2015).[7]

AB 32 added information collected from automated license plate recognition systems to the definition of protected personal information, a data breach of which would trigger a notice of breach by state and local government agencies and by businesses (effective January 1, 2016).[8]

With the 2015 iteration of data breach legislation that triggers a breach notice, the triggers for such notice now include data breaches with compromised information collected through automated license plate recognition systems.

Highlights of US Health Data Privacy and Security Legislation

HITECH Act of 2009. In 2009, the American Recovery and Reinvestment Act (ARRA) set in motion incentives for the creation of a national healthcare infrastructure to expand the adoption and use of health information technology and included incentives to accelerate the adoption of electronic health record systems among providers. The Health Information Technology for Economic and Clinical Health Act (HITECH) is part of ARRA.

HITECH key elements:

- Expansion of the scope of privacy and security protections under HIPAA—the Health Insurance Portability and Accountability Act of 1996.
- Increase of the legal liability for noncompliance, with higher monetary penalties.
- Stronger enforcement of the protection of PHI—it required the US Department of Health and Human Services (HHS) to conduct periodic PHI compliance audits of covered entities and business associates.

- Requirement of data breach notification for unauthorized uses and disclosures of "unsecured protected health information."
  - Unsecured PHI data breach notifications must be sent to patients.
  - If the breach involves 500 or more patients, the HHS secretary must be notified, in which case the breaching entity's name will be made public on HHS's website.
  - Local media need to be notified (in certain cases).

HITECH defines *breach of unsecured protected health information* as "the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information. . . ." HITECH defines *unsecured protected health information* as "protected health information that is not secured through the use of a technology or methodology specified by the [HHS] Secretary in guidance."

HITECH's Security Rule made the 2003 HIPAA security standards applicable to covered entities (i.e., health plans, healthcare providers, and so on) and business associates.[9,10]

HIPAA Omnibus Rule of 2013. HHS's HIPAA Omnibus Rule, published on January 25, 2013, set in place final regulations modifying HIPAA's privacy, security, and enforcement rules to implement various requirements of HITECH. The Omnibus Rule authorized HHS's Office of Civil Rights to enforce violations of HIPAA's privacy and security rules, defined when breaches of unsecured protected health information are to be reported to HHS, and defined the relationship between BAs and their subcontractors with regard to managing protected health information.[11,12]

HITECH—Select Definitions from Subtitle D

Breach. "… the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

Business associate. "… with respect to a covered entity, a person who:

> (i) On behalf of such covered entity or of an organized healthcare arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of [(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing]."

Covered entity. A health plan, a healthcare clearinghouse, or a healthcare provider who transmits electronically protected health information.

Protected health information. Individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium (www.hhs.gov).[10]

Reference Sources

1. SB 1386 (Cal. 2002).
2. AB 1950 (Cal. 2004).
3. Cal Civil Code § 1798.81.5.
4. AB 1298 (Cal. 2007).
5. SB 24 (Cal. 2011).
6. SB 46 (Cal. 2013).
7. AB 1710 (Cal. 2014).
8. SB 34 (Cal. 2015).
9. Health Information Technology for Economic and Clinical Health Act (2009), 42 USC 17921 et seq, www.hhs.gov (PDF).
10. US Dept. of Health & Human Services, "The Security Rule," www.hhs.gov.
11. US Dept. of Health & Human Services, New Rule Protects Patient Privacy, Secures Health Information. January 17, 2013, www.gpo.gov (PDF).
12. US Dept. of Health & Human Services, "Omnibus HIPAA Rulemaking," www.hhs.gov.

Appendix B. Web Descriptions Tables, California and US Comparisons

TABLE 1. Standardized Rates* of Types of Stolen Devices, CEs, CA and US, 2010-2015

TYPE OF DEVICE	CA	US
Desktop Computer	0.0179	0.0118
Laptop Computer	0.0179	0.0436
Portable Electronic Storage	0.0077	0.0152
Network Server	0.0051	0.0022
Total	**0.0485**	**0.0728**

TABLE 2. Standardized Rates* of Individuals Affected by Breaches of 500+ Individuals Caused by Theft According to Type of Stolen Device, CEs, CA and US, 2010-2015

TYPE OF DEVICE	CA	US
Desktop Computer	72.2752	45.6439
Laptop Computer	2,136.0196	828.3311
Portable Electronic Storage	51.1715	184.6342
Network Server	104.6396	38.1645
Total	**2,371.7699**	**1,096.7737**

TABLE 3. Standardized Rates* of Types of Stolen Devices, BAs, CA and US, 2010-2015

TYPE OF DEVICE	CA	US
Desktop Computer	0.0281	0.0034
Laptop Computer	0.0051	0.0068
Portable Electronic Storage	0.0153	0.0077
Network Server		
Total	**0.0485**	**0.0180**

TABLE 4. Standardized Rates* of Individuals Affected by Breaches of 500+ Individuals Caused by Theft According to Type of Stolen Device BAs, CA and US, 2010-2015

TYPE OF DEVICE	CA	US
Desktop Computer	168.6047	20.5339
Laptop Computer	14.4693	19.4945
Portable Electronic Storage	178.4859	103.6716
Network Server		
Total	**361.5599**	**143.5756**

TABLE 5. Standardized Rates* of Physical Locations Experiencing Device Thefts, CEs, CA and US, 2010-2015

TYPE OF PHYSICAL LOCATION	CA	US
Office	0.0204	0.0261
Vehicle	0.0102	0.0159
Residence	0.0051	0.0028
Other		0.0068
Total	**0.0358**	**0.0516**

TABLE 6. Standardized Rates* of Number of Individuals Affected by Type of Physical Location Experiencing Theft of Electronic Devices, CEs, CA and US, 2010-2015

TYPE OF PHYSICAL LOCATION	CA	US
Office	1,955.8936	744.6773
Vehicle	216.8384	105.0265
Residence	86.8978	40.0372
Other		71.5870
Total	**2,259.6299**	**961.3280**

*Standardized rates of stolen devices from Web Descriptions are per 100,000 population and based on 2015 population estimates of California and US (www.census.gov/quickfacts). Rates are computed by the author.

Note: No Business Associates data for Tables 5 and 6. See section starting on page 12 for more information.

Data source for all tables: US Dept. of Health & Human Services, Office of Civil Rights, Breaches Affecting 500 or More Individuals.

Business Associates: Standardized Rates of Types of Physical Locations of Thefts and Individuals Affected by Type of Physical Location Experiencing Theft of Electronic Devices, 2010-2015

Comparison of types and rates of physical locations of stolen devices and individuals affected as reported by US and California Business Associates (no tables):

- California Business Associates' offices, as a type of physical location in which theft of electronic devices occurred, had a standardized rate (0.0052 offices per 100,000 population) higher than that of the national average (0.0025 offices per 100,000 population).
  - In California, more Business Associate offices experienced theft of electronic devices with unsecured protected health information than similar thefts from Business Associate offices in the United States.
- California's Business Associates' vehicles, as a type of physical location in which theft of electronic devices occurred, had a standardized rate (0.0077 vehicles per 100,000 population) higher than that of the national average rate (0.0037 vehicles per 100,000 population).
- Rates for other types of physical location among California Covered Entities were lower than the national average.
- Overall, California Business Associates' physical locations identified in the Web Description section of HHS data constituted a higher rate of type of physical location per 100,000 population (0.0128) than the US average (0.0121).
- Theft of electronic devices from California Business Associates' offices impacted a higher rate of individuals (168.6047 individuals affected per 100,000 population) than the US average (26.3765 individuals affected per 100,000 population. Thefts of electronic devices from California Business Associates' offices affect individuals at a rate 6.39 times higher than the US average rate.

Findings from Analysis of Web Descriptions: Breaches of Unsecured Protected Health Information Caused by Theft in California and the US, 2010-2015

Findings reported in this section were derived from an in-depth analysis of text available in certain descriptions in the Web Description section of the HHS database for data years 2010-2015 describing details of thefts.

Table 1. Comparison of types and rates of stolen devices reported by US and CA Covered Entities:

- Between 2010 and 2015 California's Covered Entities experienced a higher rate of desktop computer thefts (0.0179 thefts per 100,000 population) than the national average (0.0118 thefts per 100,000 population).
- Similarly, California Covered Entities experienced a higher theft rate of network servers (0.0051) than the US average (0.0022).

Table 2. Comparison of rates of individuals affected from the theft of electronic devices reported by US and CA Covered Entities:

- Thefts of electronic devices reported by California's Covered Entities impacted higher rates of individuals (per 100,000 population) than the national average according to the following types of stolen devices reported in the Web Description section of the HHS database:
  - *Desktop computers*: CA 72.2752 individuals affected per 100,000 population versus US 45.6435 individuals affected.
  - *Laptop computers*: CA 2,136.0196 individuals affected per 100,000 population versus US 828.3311 individuals affected.
  - *Network servers*: CA 104.6396 individuals affected per 100,000 population versus US 38.1645 individuals affected.
- Overall, these findings point to the following trends:
  - The theft of electronic devices from California Covered Entities has impacted more than twice as many individuals than the national average.
  - Thefts of laptop computers reported by California Covered Entities have impacted more than twice

as many individuals than the national average for the 2010-2015 reporting years.

- Theft of network servers reported by California Covered Entities has impacted individuals at a rate nearly three times higher than the national average.

Table 3. Comparison of types and rates of stolen devices reported by US and CA Business Associates:

- California's Business Associates experienced a rate of desktop computer thefts (0.0281 desktop computer thefts per 100,000 population) that was 8.26 times higher than the national average (0.0034 thefts per 100,000 population).
- California Business Associates experienced a higher theft rate of portable electronic storage devices (0.0153) than the US average (0.0077).
- Overall, California Business Associates experienced a rate of theft (0.0485) for all types of devices 2.69 times higher than the national average (0.0180).

Table 4. Comparison of rates of individuals affected from the theft of electronic devices reported by US and CA Business Associates:

- Thefts of electronic devices reported by California's Business Associates impacted higher standardized rates of individuals (per 100,000 population) than the national average according to the following types of stolen devices reported in the Web Description section of the HHS database:
  - *Desktop computers*: CA 168.6047 individuals affected per 100,000 population versus US 20.5339 individuals affected.
  - *Portable electronic storage*: CA 178.4859 individuals affected per 100,000 population versus US 103.6716 individuals affected.
- Overall, the theft of electronic devices from California Business Associates has impacted 2.52 times more individuals than the national average.
- Thefts of desktop computers reported by California Business Associates have impacted 8.21 times more individuals (168.6047 individuals per 100,000 population) than the national average (20.5339 individuals per 100,000 population) for the 2010-2015 reporting years.

Table 5. Comparison of types and rates of physical locations of stolen devices reported by US and CA Covered Entities:

- California Covered Entities' residences were the only type of physical location that had a standardized rate (0.0051 residences per 100,000 population) higher than that of the national average rate (0.0028 residences per 100,000 population).
  - That is, in California, more Covered Entity–associated residences experienced theft of electronic devices with unsecured protected health information than similar thefts from Covered Entity–associated residences in the United States.
- Rates for other types of physical location among California Covered Entities were lower than the national average.
- Overall, California Covered Entities' physical locations identified in the Web Description section of HHS data constituted a lower rate of theft by type of physical location involved type of physical location per 100,000 population (0.0358) than the US average (0.0516).

Table 6. Comparison of rates of individuals affected from the theft of electronic devices according to the type of physical location experiencing such theft reported by US and CA covered entities:

- Thefts of electronic devices that occurred in California Covered Entities' offices affected individuals at higher rates (1,955.8936 per 100,000 population) than the national average for similar physical location (744.6773).
  - California's rate was 2.63 times higher than the national average.
- Thefts of electronic devices that occurred in vehicles of California's Covered Entities affected a higher rate of individuals (216.8384 per 100,000 population) than the national average for vehicles (105.0265).
  - California's rate was 2.06 times higher than the national rate for this type of physical location.
- Thefts of electronic devices that occurred to California's Covered Entities' residences affected a higher rate of individuals (86.8978) than the national average for the same type of physical location (40.0372).

- California Covered Entities' rate of affected individuals from this type of physical location of theft was 2.17 times higher than the national average for the same physical location.

- Overall, the average rate of individuals affected (2,259.6299 per 100,000 population) from California Covered Entities' thefts from three types of physical locations (office, vehicle, and residence) was 2.35 times higher than the national average of 961.3280 affected individuals per 100,000 population.

  - The US national average also includes the physical location "Other," with a rate of 71.5870 affected individuals per 100,000 population; California did not report any occurrences of thefts of electronic devices from this type of physical location. "Other" refers to physical locations such as in transportation/shipping, US mail, and private delivery companies.

Data Resources and Considerations

Data Resources

US Department of Health & Human Services, Breaches Affecting 500 or More Individuals.

State of California Legislative Counsel, California Legislative Information.

Data Considerations

1. Some minimal duplication of cases may have occurred due to HHS's website reporting system.

2. A number of entries (fewer than 10) were eliminated from inclusion in the analysis of data years 2010-2015 due to lack of identifiable information such as year of reporting and state.

3. Although the HHS website reports data on breaches of unsecured protected health information from 2009 to 2016, only the period of 2010-2015 contains complete annual data. Therefore, only the years 2010-2015 are included in the present analysis.

4. Web Description analysis considerations: For reasons that are beyond the scope of this investigation, it is noted that the HHS portal reporting breaches of unsecured protected health information affecting 500 or more individuals does not include a text description in its Web Description section for all breaches caused by theft. Details follow:

- Among US Business Associates reporting theft as the cause of breach (*n*=109), 55.04% of theft reports were accompanied by text in the Web Description section of the database and therefore analyzed by this investigation.

- Among US Covered Entities reporting theft as the cause of breach (*n*=544), 47.43% of reported thefts were accompanied by text in the Web Description section.

- Among California Business Associates reporting theft (*n*=15), 46.67% of theft reports were accompanied by text in the Web Description of the database.

- Among California Covered Entities reporting theft as the cause of breach (*n*=77), 25.97% of theft reports were accompanied by text in the Web Description of the database.

Because of the limited availability of text description of thefts in the Web Description section of the HHS database, the analysis used standardized comparisons per 100,000 population (US Census Bureau, 2015 population estimates).

The standardized rate of the number of incidents (e.g., number of devices stolen, number of individuals affected by stolen devices, physical locations, or work roles) was derived by dividing the number of incidents by the US Census 2015 population estimate for California or the US, and multiplying the result by 100,000.

US and CA Covered Entities and Business Associates—Total Number of Breaches and Individuals Affected

See page 15 for tables.

TABLE 7. Total Number of Breaches and Individuals Affected, by Type of CE and BA United States, 2010-2015

	BREACHES		INDIVIDUALS AFFECTED	
	NUMBER	% OF TOTAL	NUMBER	% OF TOTAL
Health Plan*	158	11.50%	107,692,623	70.55%
Healthcare Clearing House	4	0.29%	17,754	0.01%
Healthcare Provider†	945	68.78%	20,065,460	13.15%
Business Associates	267	19.43%	24,863,652	16.29%
Total	**1,374**	**100.00%**	**152,639,489**	**100.00%**

*Health Plan breaches account by far for the largest percentage of individuals affected (70.55%) during the 2010-2015 data period.

†While breaches reported from Healthcare Providers (a subcategory of Covered Entities experiencing 68.78% of all breaches) affected 13.15% of the total number of individuals affected by all breaches, Business Associates' breaches (with 19.43% of all breaches) affected a higher percentage of individuals (16.29%) than those affected by Healthcare Providers during the 2010-2015 data period.

TABLE 8. Total Number of Breaches and Individuals Affected, by Type of CE and BA California, 2010-2015

	BREACHES		INDIVIDUALS AFFECTED	
	NUMBER	% OF TOTAL	NUMBER	% OF TOTAL
Health Plan	13	10.15%	157,705	2.27%
Healthcare Clearing House	0	0.00%	0	0.00%
Healthcare Provider*	109	85.16%	6,765,503	97.25%
Business Associates†	6	4.69%	33,523	0.48%
Total	**128**	**100.00%**	**6,956,731**	**100.00%**

*In California, Healthcare Providers (a subcategory of Covered Entities) account both for the largest percentage of breaches (85.16%) and the largest percentage of individuals affected (97.25%) during the 2010-2015 data period.

†California Business Associates accounted for 4.69% of all California breaches and 0.48% of all individuals affected. Findings from the comparison between California Healthcare Providers and California Business Associates suggest the presence of a trend that is opposite to national-level findings shown in Table 7. At the national level, Business Associates experienced 19.43% of all breaches and affected a higher percentage of individuals (16.29%) than those impacted by Healthcare Providers during the 2010-2015 data period (Table 7).

Data source for all tables: US Dept. of Health & Human Services, Office of Civil Rights, Breaches Affecting 500 or More Individuals.

Appendix C. Conclusion Details

This investigation recognizes that, in part because the HHS database on breaches of unsecured protected health information affecting 500 or more individuals is constantly updated, additional research is required on such breaches, especially those impacting California. Nevertheless, a number of policy-relevant findings and trends have emerged from the analysis conducted thus far.

Business Associates are more vulnerable than CEs—in CA and US. Among US Covered Entities and Business Associates, breaches reported from Business Associates have affected more individuals than those from Healthcare Providers (13% among Healthcare Providers versus 16% among Business Associates—see Table 7 in Appendix B). While this finding pertains only to the comparison between Healthcare Providers and Business Associates and not between all Covered Entities and Business Associates, it may echo the comments of HHS Secretary Kathleen Sebelius, who upon announcing HHS's HIPAA Omnibus Rule of 2013, observed that some of the largest breaches in the US have been reported by Business Associates.

Theft is a major area of vulnerability. Theft as a cause of breaches among California's Covered Entities and Business Associates is higher than that of their respective counterparts at the national level (theft for CA Covered Entities is 12 percentage points higher than their national counterparts; theft for CA Business Associates is 8 percentage points higher than nationally). Theft (all theft) makes for the largest category of breaches in the United States and in California.

California CEs have higher rates of desktop computer and network server theft than the rest of the US. The in-depth analysis of text from Web Descriptions accompanying theft (as a Type of Breach or cause of breach) generated several policy-relevant findings expressed as standardized rates (rates): (a) California's Covered Entities experienced a higher rate of desktop computer thefts (0.0179 thefts per 100,000 population) than the national average (0.0118 thefts per 100,000 population); (b) California Covered Entities experienced a higher theft rate of network servers (0.0051) than the US average (0.0022). Overall, the theft of all electronic devices among California's Covered Entities (a) has impacted more than twice as many individuals than the national average; (b) thefts of laptop computers reported by California Covered Entities have impacted more than twice as many individuals than the national average for the 2010-2015 reporting years; (c) thefts of network servers reported by California Covered Entities have impacted individuals at a rate nearly three times higher than the national average.

California BAs have higher rates of desktop and portable electronic storage device theft than the rest of the US. The in-depth analysis of text from Web Descriptions accompanying theft reported by Business Associates revealed a number of policy-relevant findings: (a) California Business Associates experienced a rate of desktop computer thefts that was 8.26 times higher than the national average; (b) California Business Associates experienced a theft rate of portable electronic storage devices that was two times higher than the US average; (c) overall, California Business Associates experienced a rate of theft for all types of electronic devices 2.69 times higher than the national average. In addition, the analysis considered the standardized rate of impacted individuals from devices stolen from Business Associates in California and the US, and found that the theft of electronic devices in California has impacted 2.52 times more individuals than the national average. More importantly, however, the analysis of Web Descriptions points to a disturbing finding: Thefts of desktop computers reported by California Business Associates have impacted 8.21 times more individuals (168.6047 individuals per 100,000 population) than the national average (20.5339 individuals per 100,000 population) for the 2010-2015 reporting years.

California BA offices are more vulnerable to theft. California's Business Associate offices, as a type of physical location in which theft of electronic devices occurred, had a standardized rate (0.0052 offices per 100,000 population) two times higher than the national average (0.0025 offices per 100,000 population). A similar trend occurred for rates of theft from Business Associate vehicles (California Business Associate vehicles were vandalized for theft of electronic devices at a rate twice that of the US). However, the rate of individuals affected by Business Associate thefts of electronic devices occurring in offices was 6.39 times higher for California Business Associates (168.6047 individuals affected per 100,000 population) than the US (26.3765 individuals affected per 100,000 population).