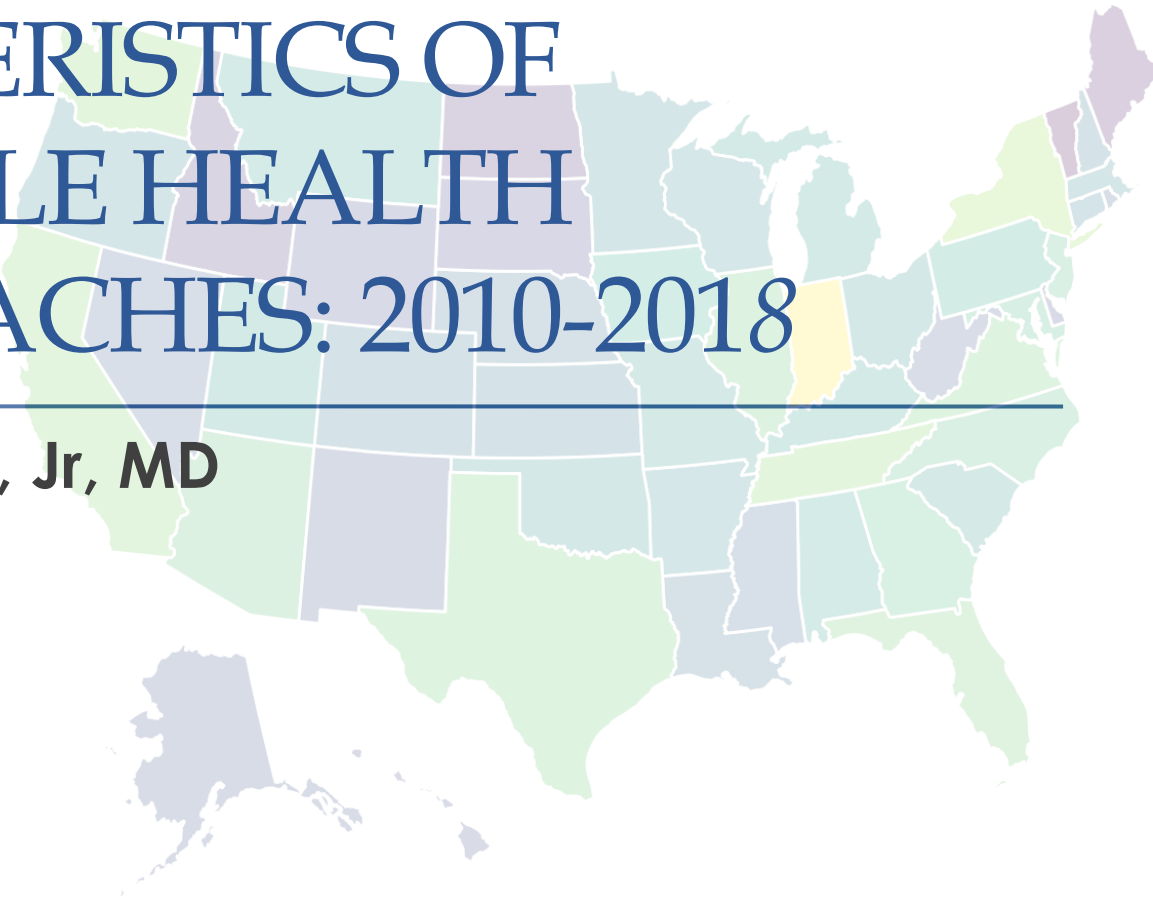


# CHARACTERISTICS OF REPORTABLE HEALTH DATA BREACHES: 2010-2018

**Thomas H. McCoy, Jr, MD**

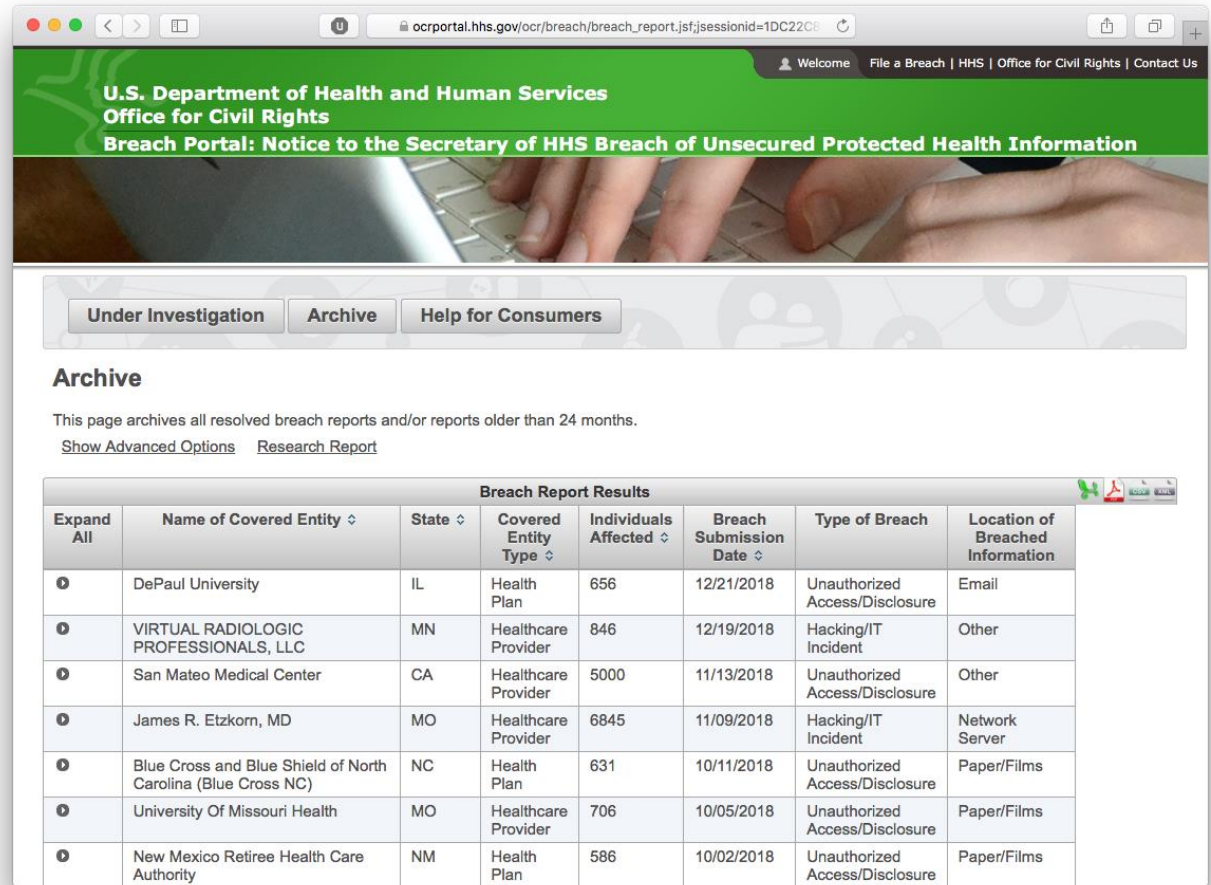
HIPAA Summit

March 5, 2019



# Public Data

OCR Breach Portal for  
500+ person breaches



The screenshot shows the OCR Breach Portal website. The header includes the U.S. Department of Health and Human Services Office for Civil Rights logo and the title "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information". Below the header are navigation buttons for "Under Investigation", "Archive", and "Help for Consumers". The "Archive" section is active, displaying a message that the page archives all resolved breach reports and/or reports older than 24 months. There are links for "Show Advanced Options" and "Research Report". The main content is a table titled "Breach Report Results" with 8 columns: Expand All, Name of Covered Entity, State, Covered Entity Type, Individuals Affected, Breach Submission Date, Type of Breach, and Location of Breached Information. The table contains 7 rows of data.

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
1	DePaul University	IL	Health Plan	656	12/21/2018	Unauthorized Access/Disclosure	Email
1	VIRTUAL RADIOLOGIC PROFESSIONALS, LLC	MN	Healthcare Provider	846	12/19/2018	Hacking/IT Incident	Other
1	San Mateo Medical Center	CA	Healthcare Provider	5000	11/13/2018	Unauthorized Access/Disclosure	Other
1	James R. Etzkorn, MD	MO	Healthcare Provider	6845	11/09/2018	Hacking/IT Incident	Network Server
1	Blue Cross and Blue Shield of North Carolina (Blue Cross NC)	NC	Health Plan	631	10/11/2018	Unauthorized Access/Disclosure	Paper/Films
1	University Of Missouri Health	MO	Healthcare Provider	706	10/05/2018	Unauthorized Access/Disclosure	Paper/Films
1	New Mexico Retiree Health Care Authority	NM	Health Plan	586	10/02/2018	Unauthorized Access/Disclosure	Paper/Films

## Elements in OCR Database

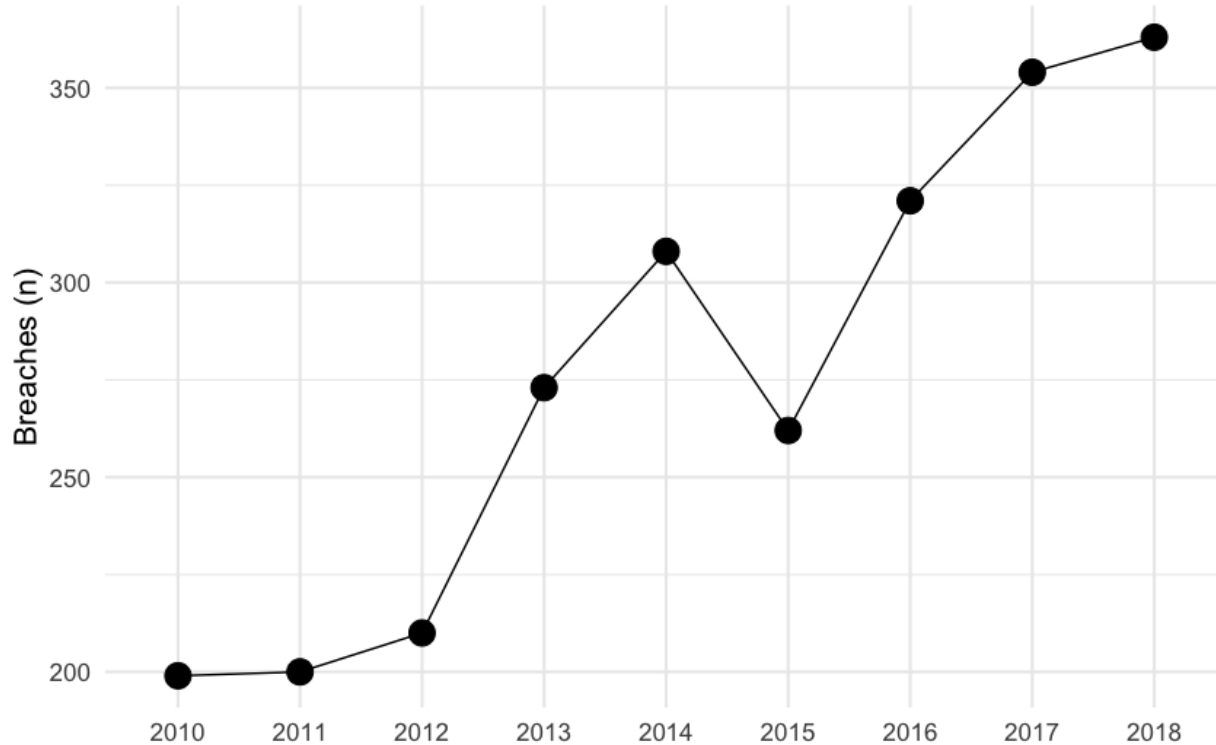
Public data includes a  
limited set of fields

- **Who:** CE type
- **What:** Number affected
- **Where:** State
- **When:** Date (reported)
- **How:**
  - *Media* - EHR, email, paper, ...
  - *Type* – Hacking, theft, loss, ...

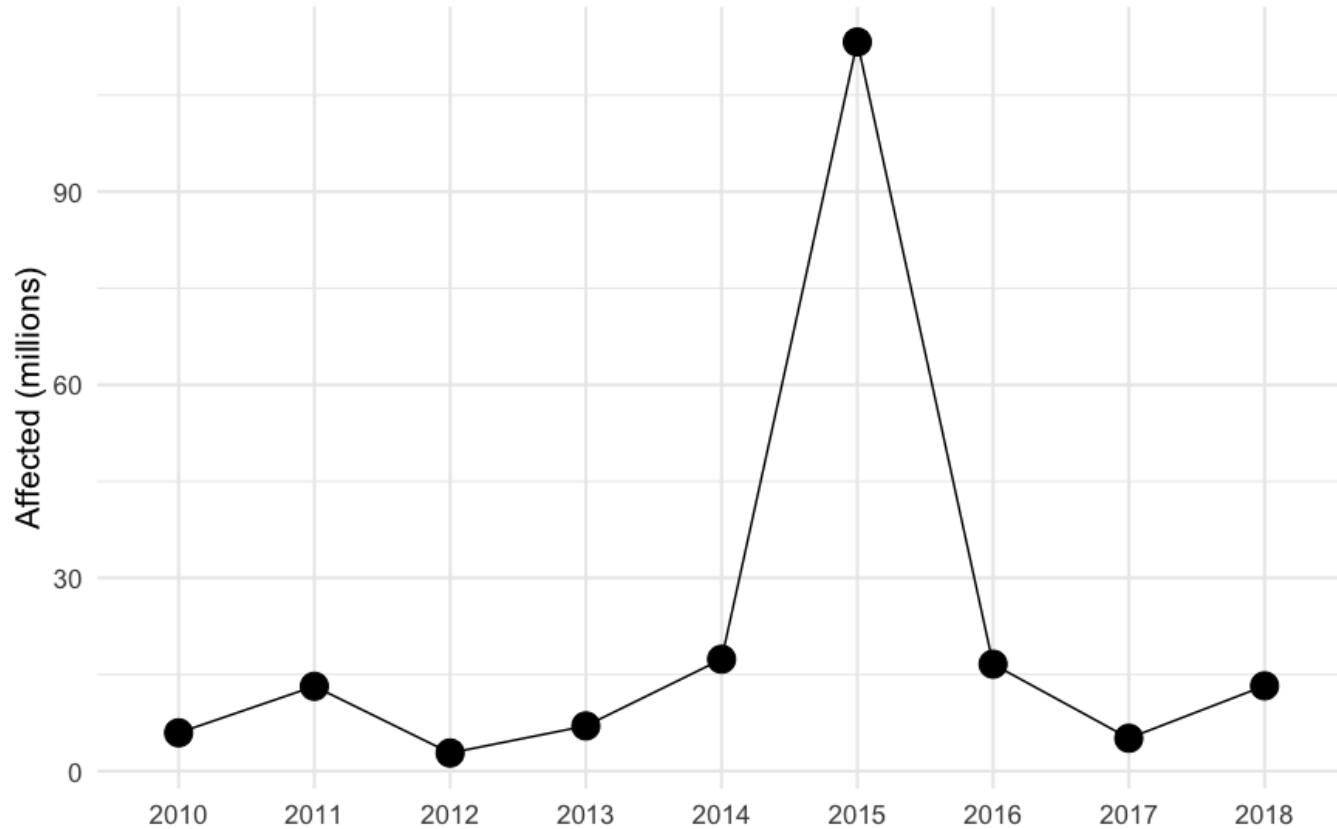
## "Outcomes"

- **Breaches** reported
  - ~ events
- **Records** affected
  - ~ people

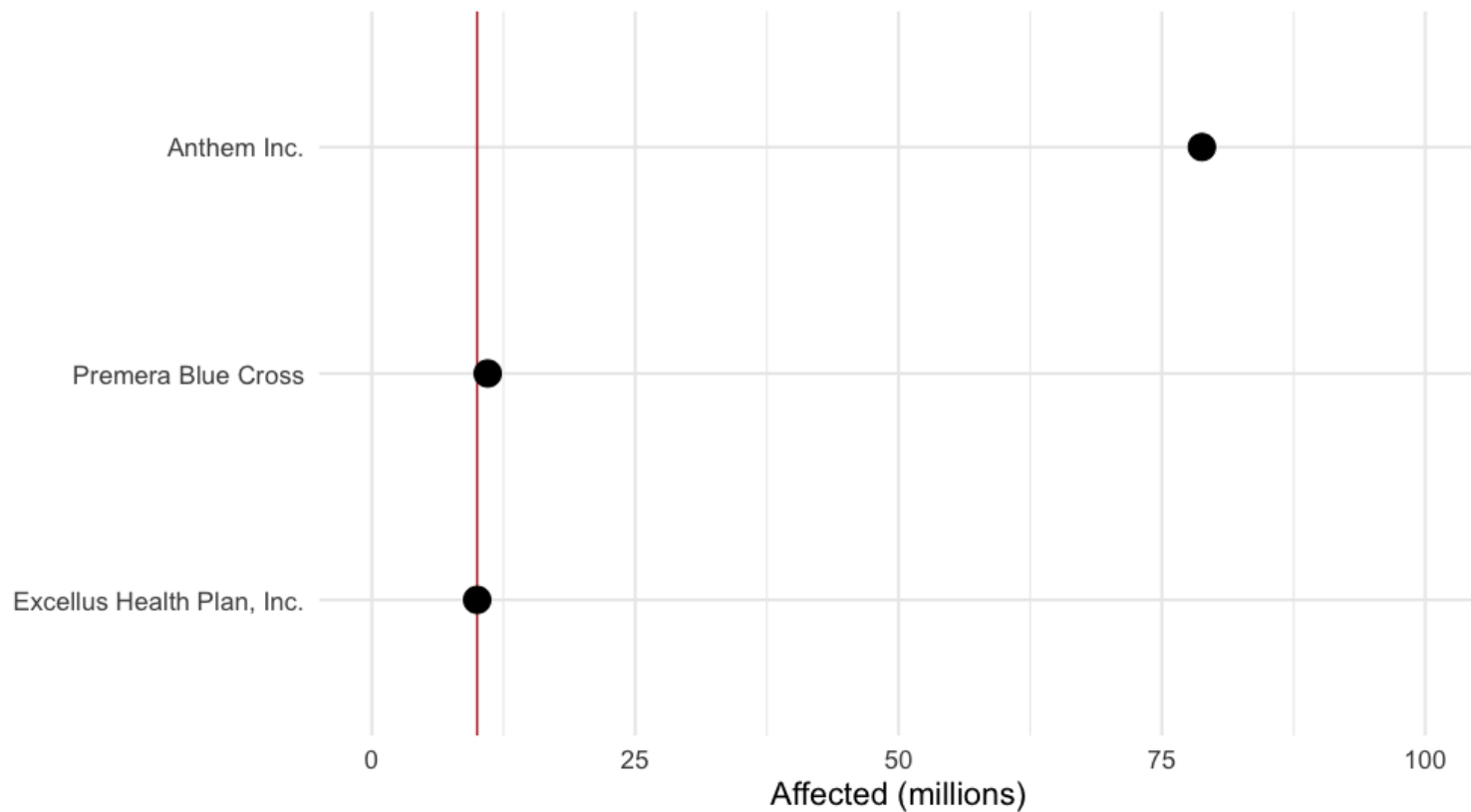
# Breaches Reported 2010-2018: 2,490



# Records Breached 2010-2018: *194.4M*



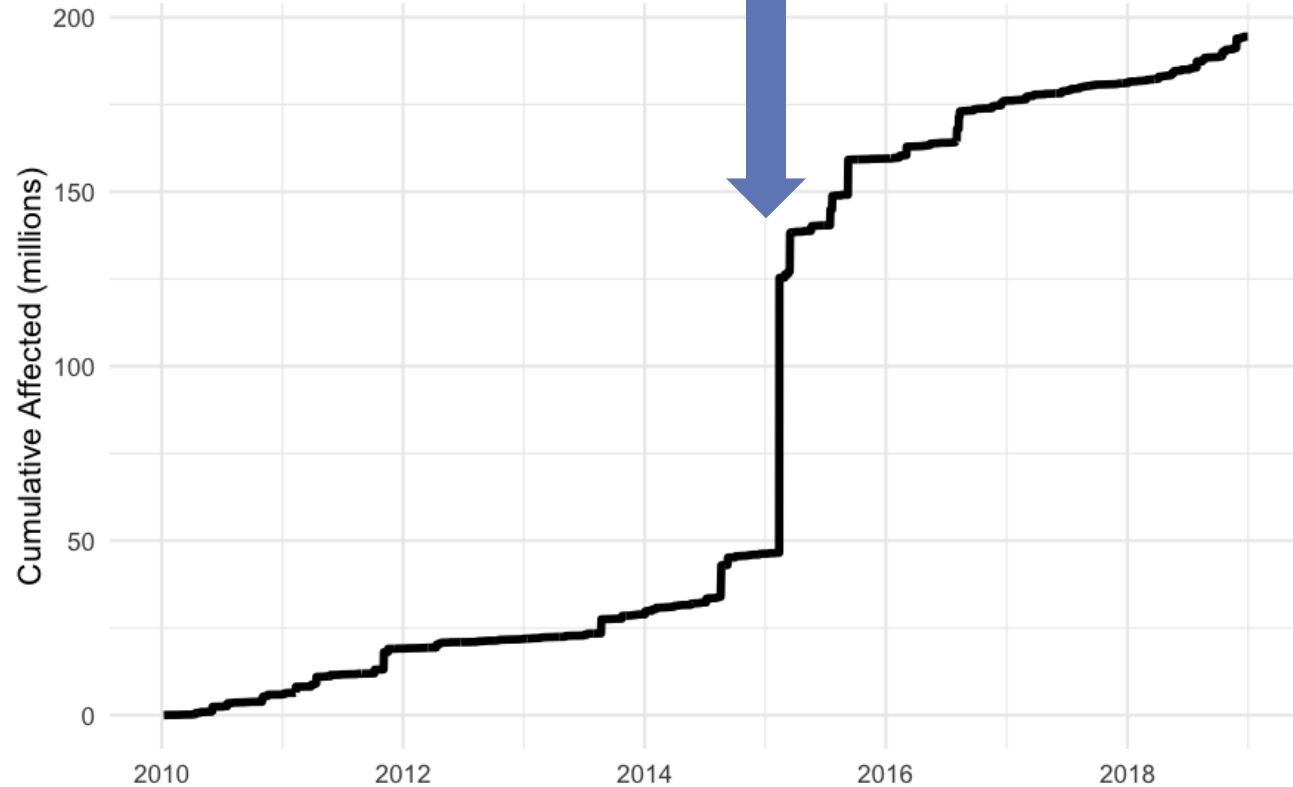
# 10M + Affected = 50% (99.8M of 194.4M)



# Cumulative affected

Digital enables perfect perpetual copies...

n.b. Likely includes some individuals multiple times.

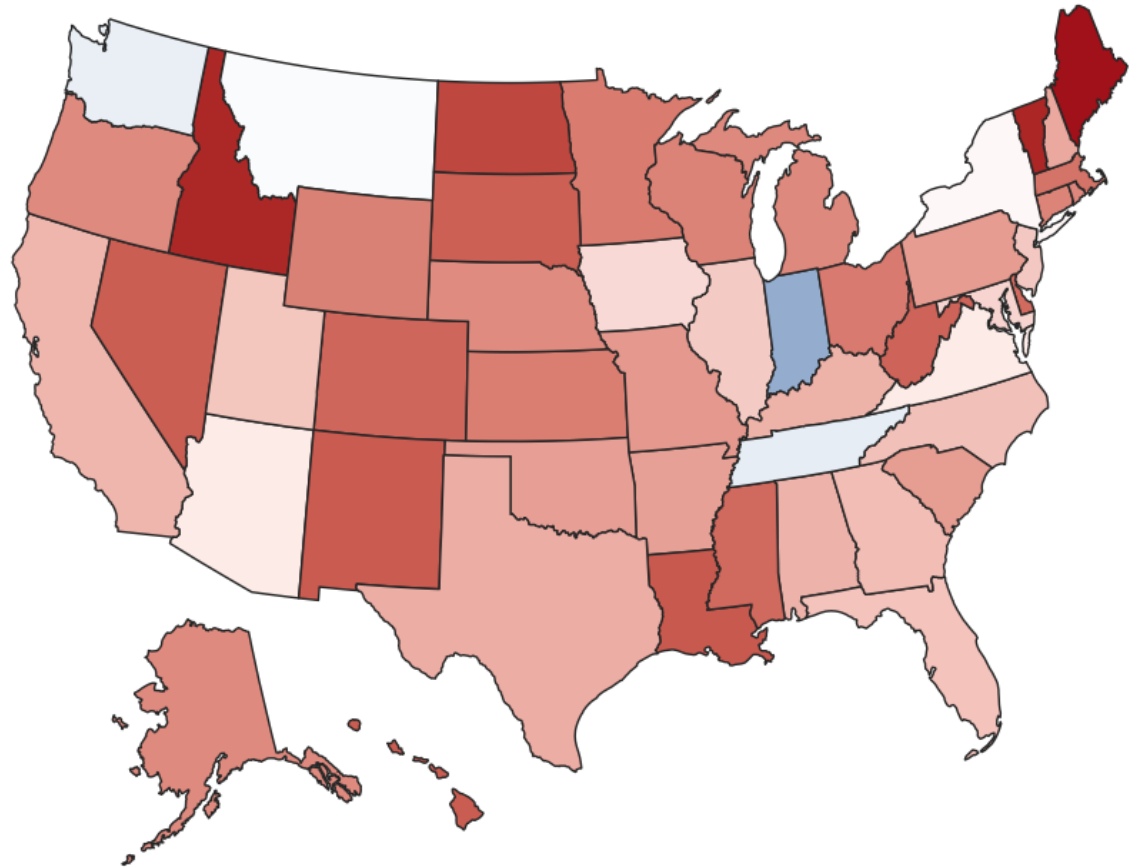
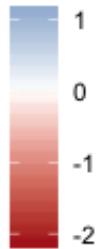




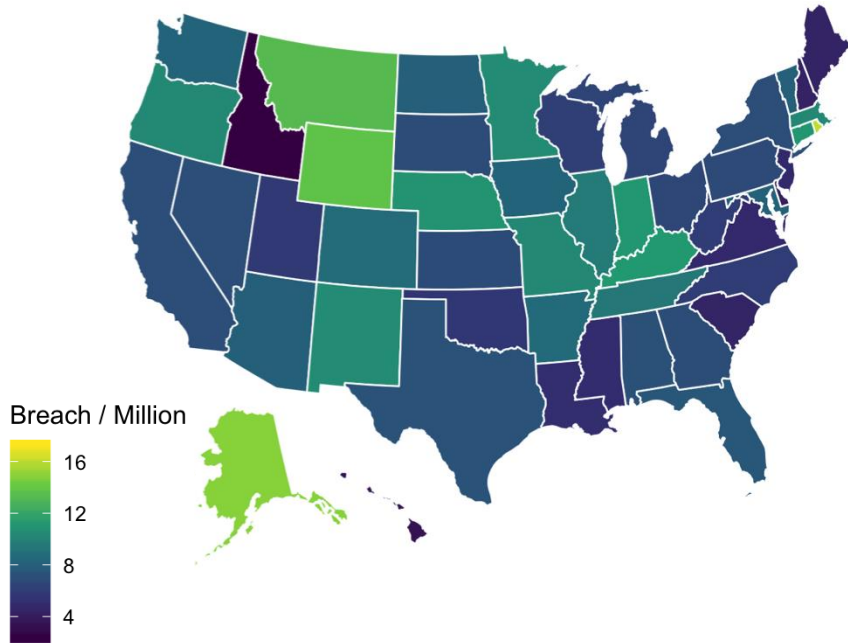
## Affected per state

Log of breached records / population  
of state, 2010-2018

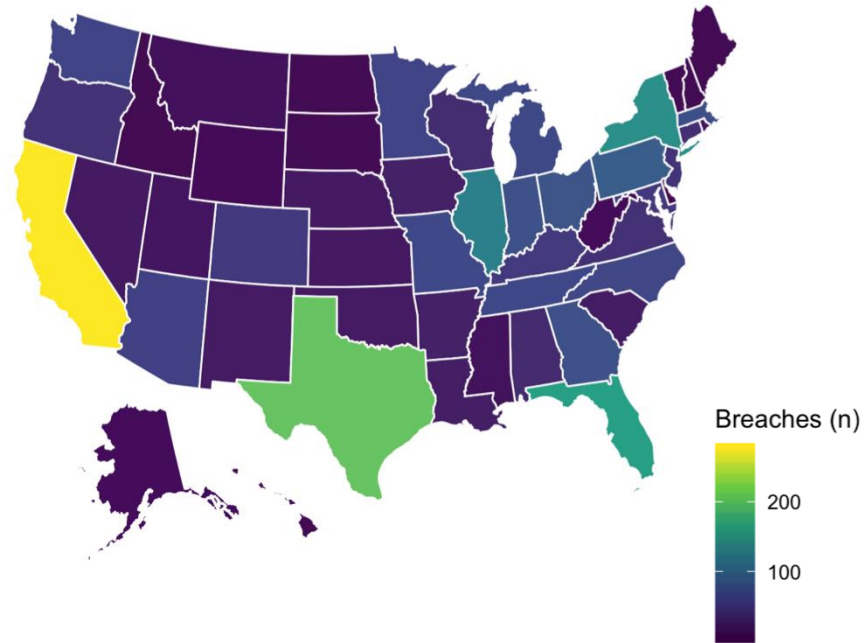
Affected / Population, log



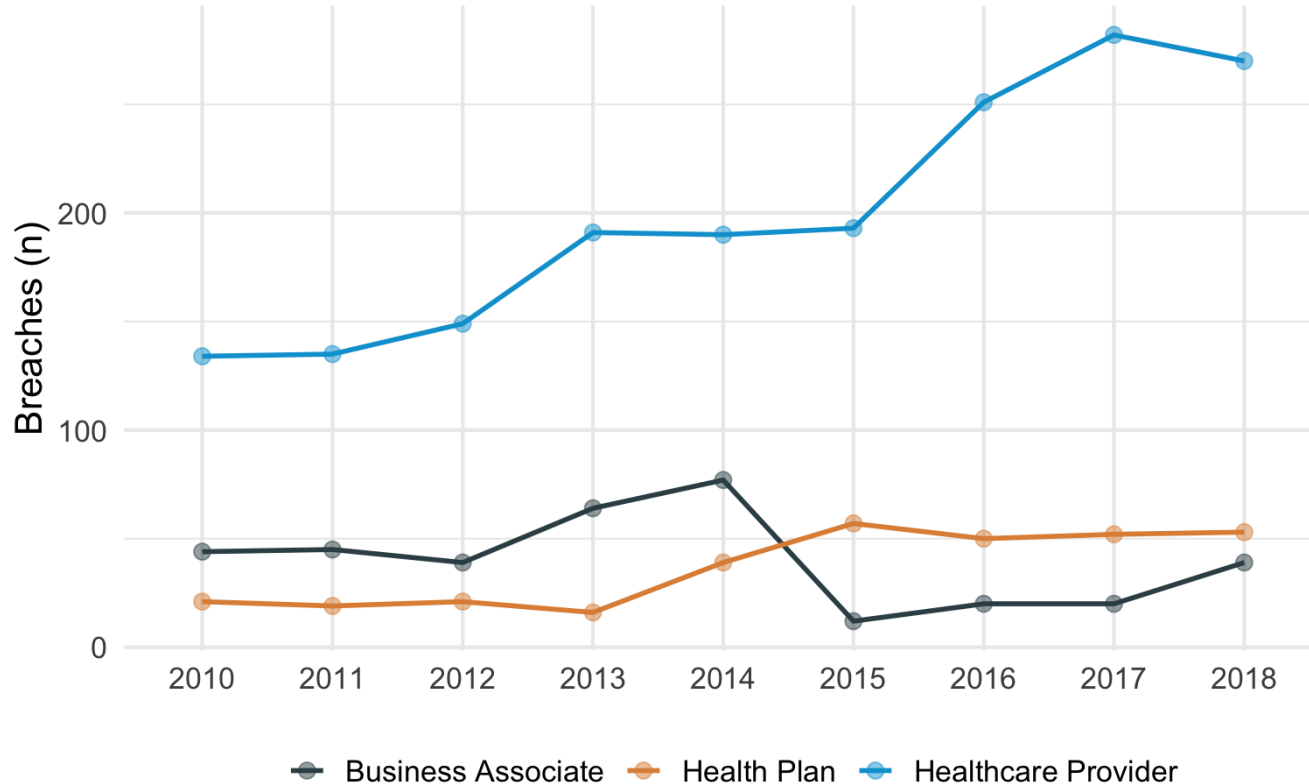
# Breaches per million



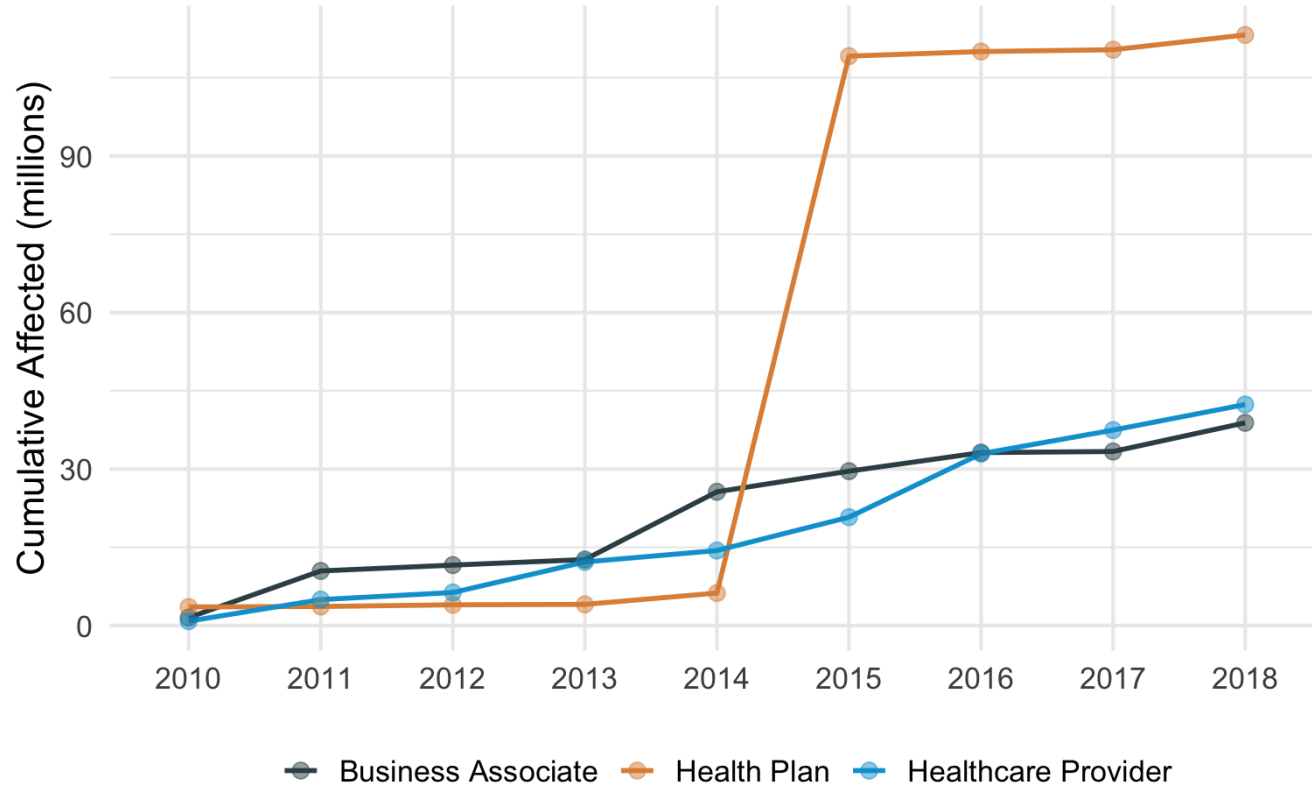
# Breaches (n)



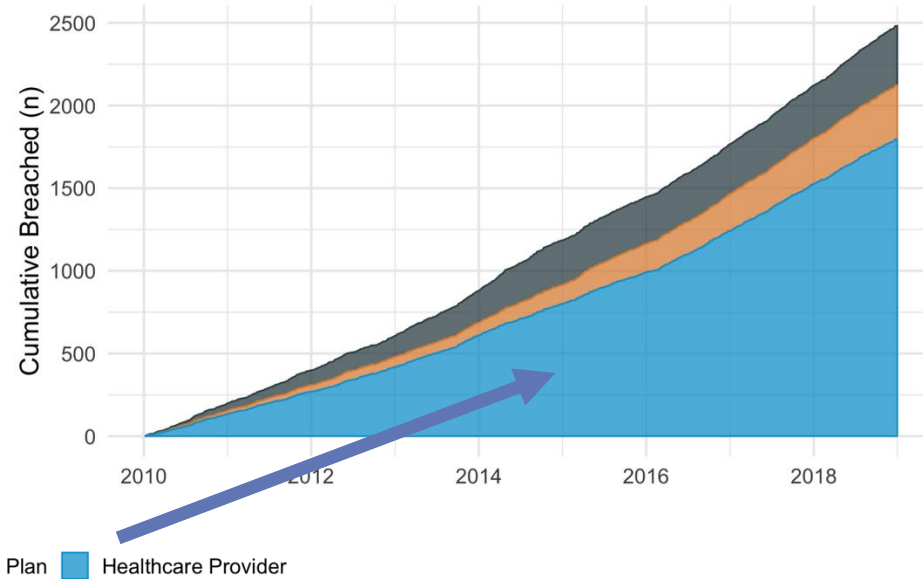
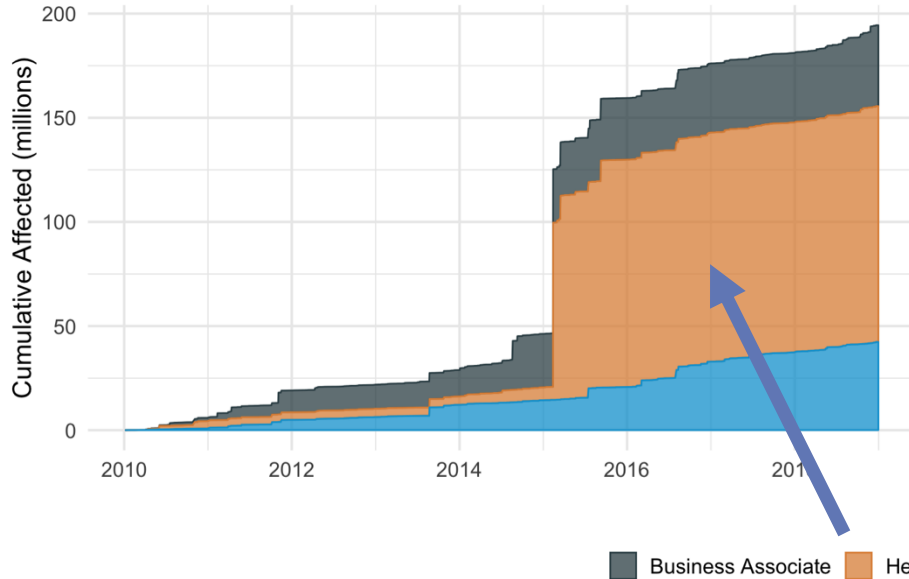
# Reported breaches by type of CE



# Cumulative affected by type of CE



# Total Affected vs Breached by CE

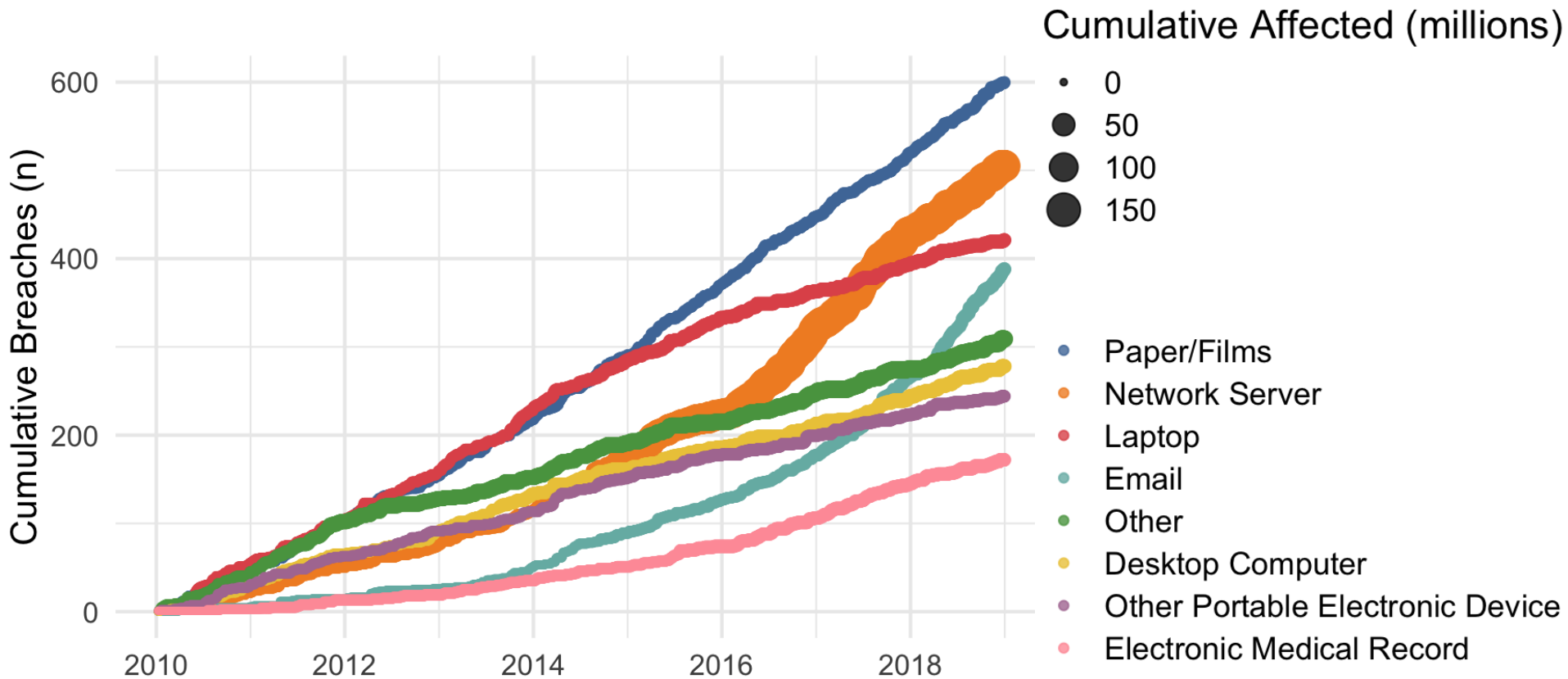


# HOW IT HAPPENED

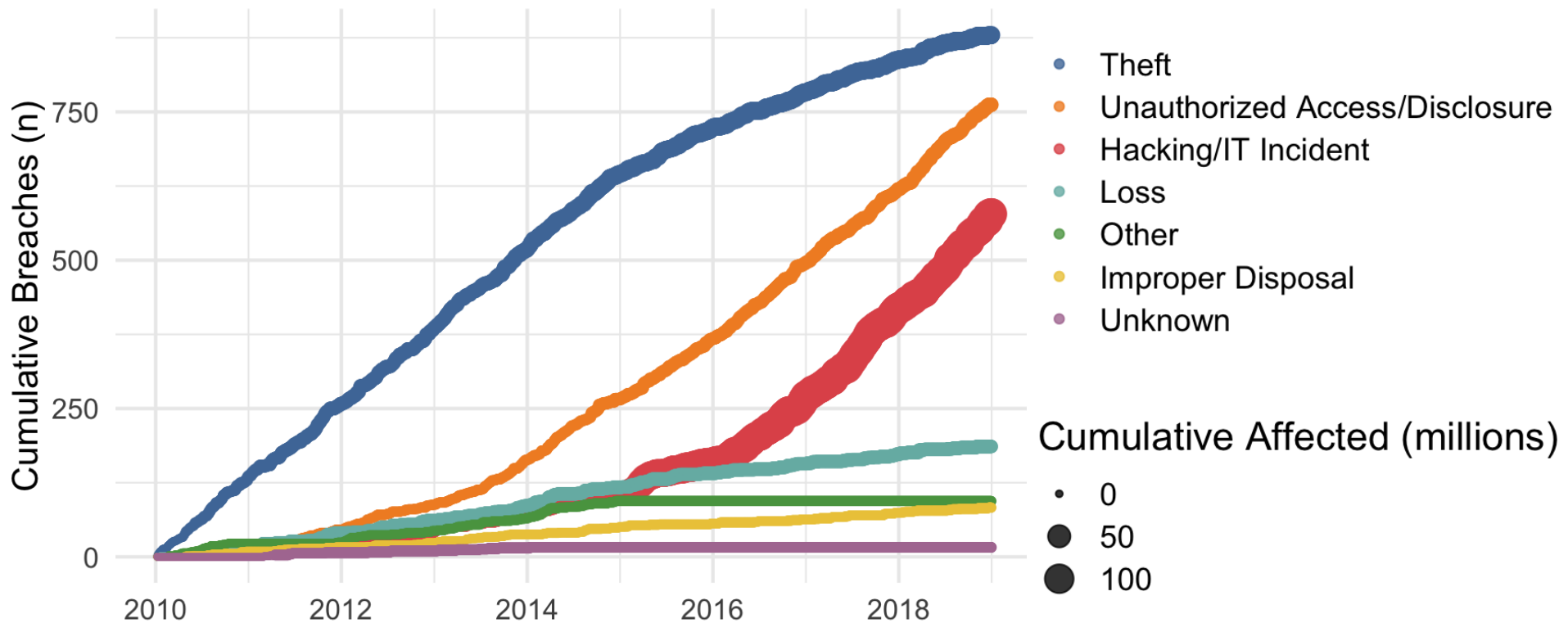
---

Moving from scope to source (or as close as we can get) of problem.

# Breaches by media location



# Breaches by event type

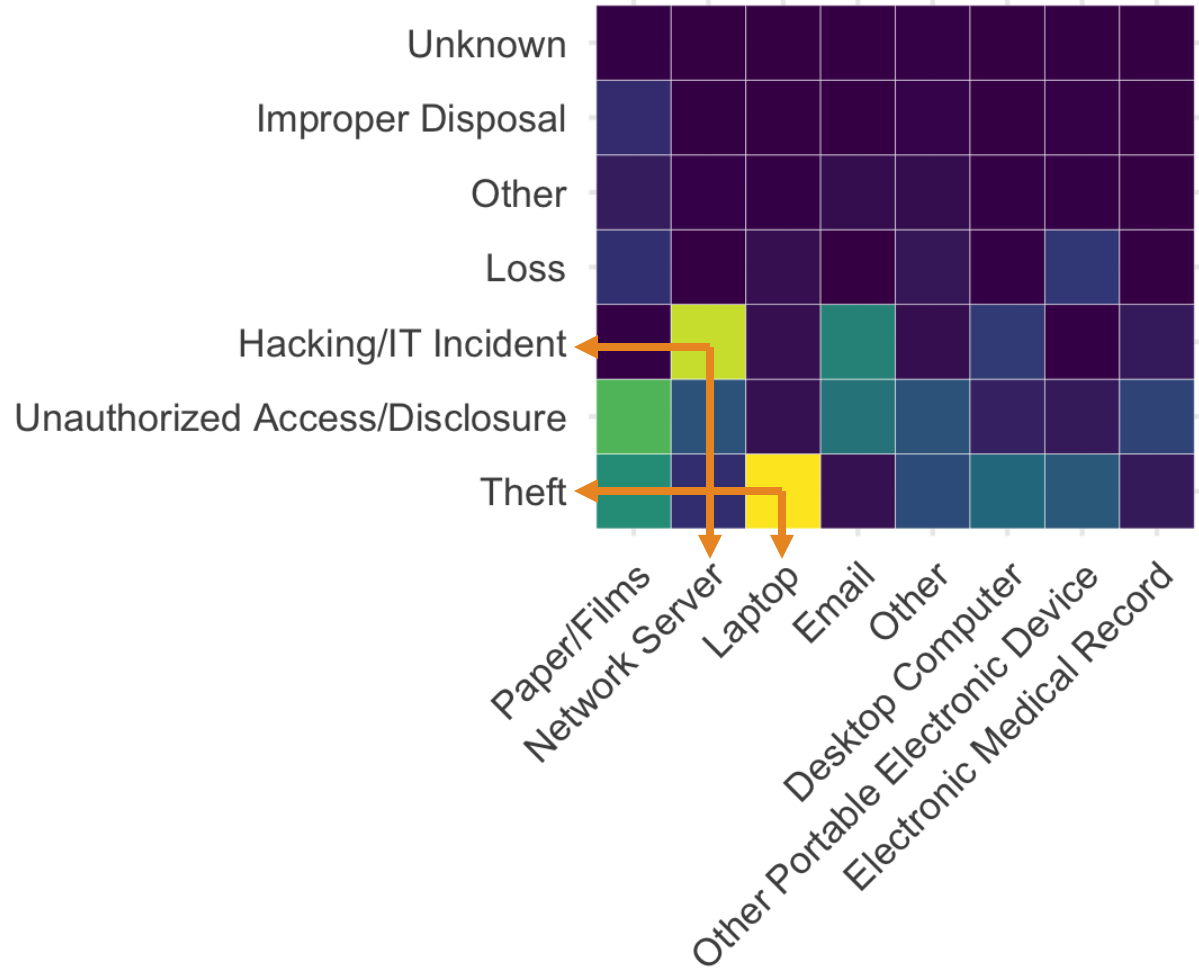
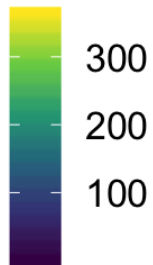




# Media location vs Event type

Laptop theft  
Server hacking

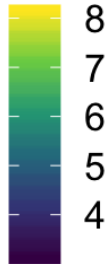
Breaches (n)



# Media location vs Event type

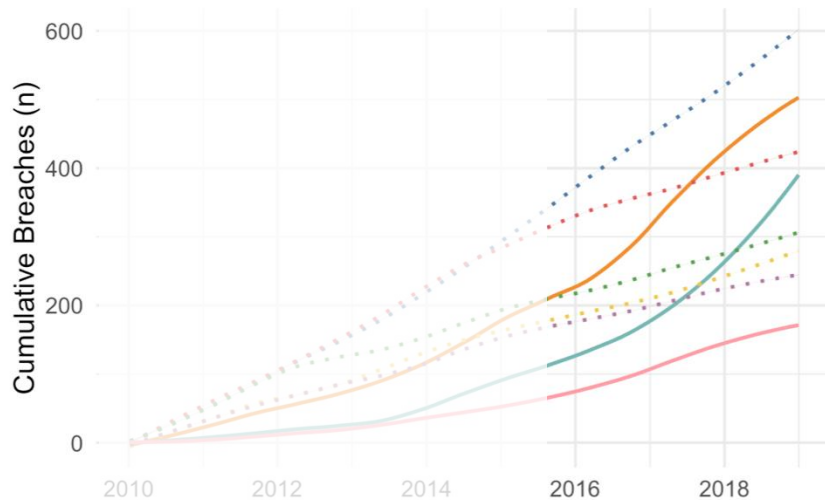
Server hacking

Affected, log

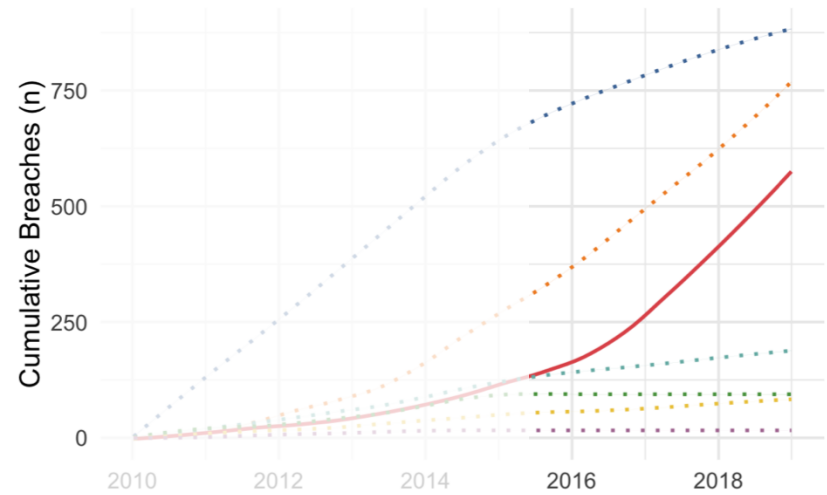


# Changes in location and type in time

## Media location



## Event type

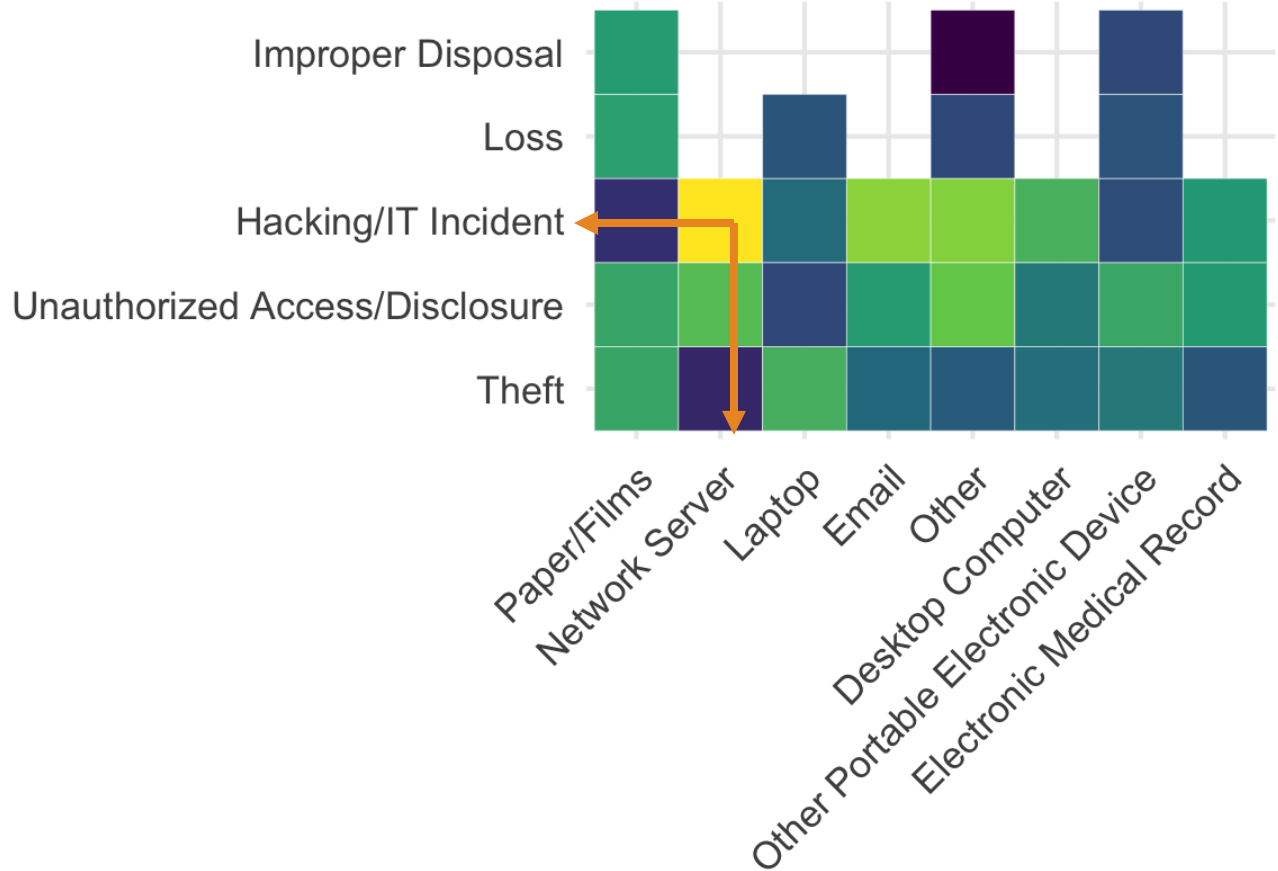
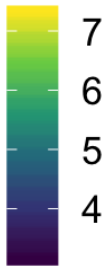




# Media location vs Event type

Server hacking

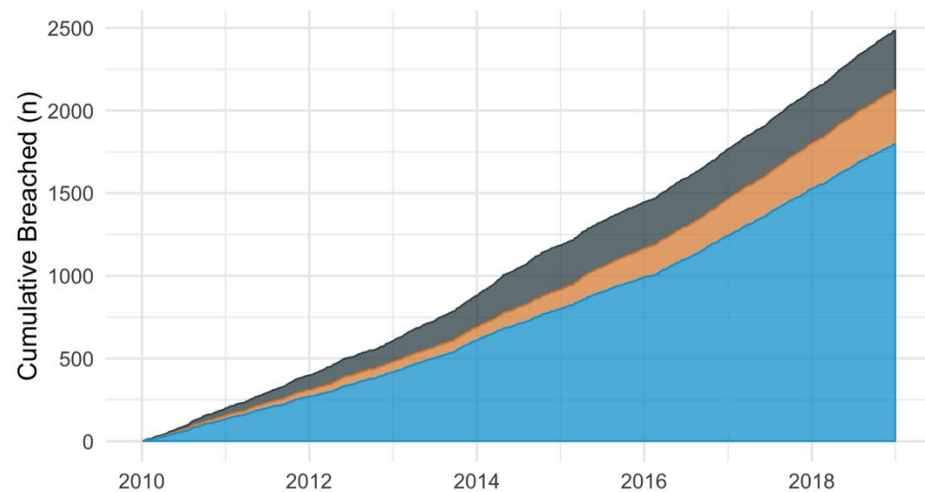
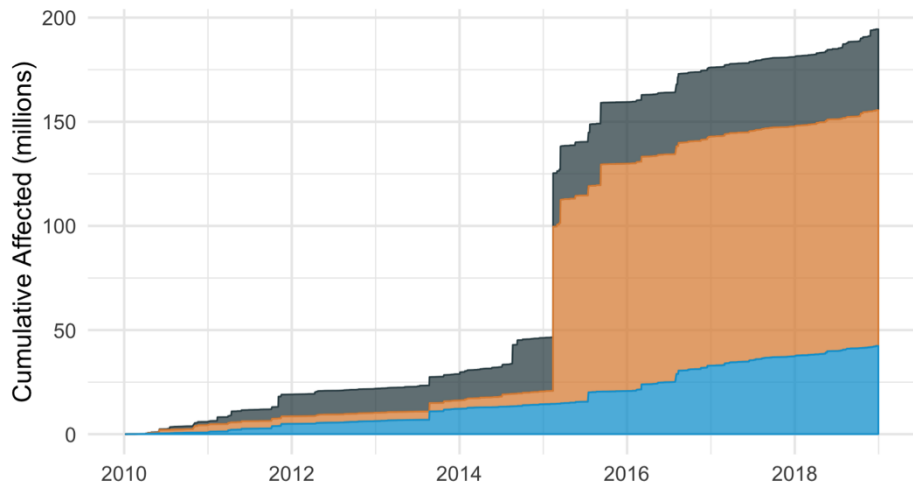
Affected, log



# FUTURE DIRECTIONS & FURTHER READING

---

# Events or records?



■ Business Associate ■ Health Plan ■ Healthcare Provider

# Thank you

Further reading:

Lui *et al* JAMA 2015

McCoy *et al* JAMA 2018



## RESEARCH LETTER

### Data Breaches of Protected Health Information in the United States

Reports of data breaches have increased during the past decade.<sup>1,2</sup> Compared with other industries, these breaches are estimated to be the most costly in health care; however, few studies have detailed their characteristics and scope.<sup>3</sup>

**Methods** | We evaluated an online database maintained by the US Department of Health and Human Services describing data breaches of unencrypted protected health information (ie, individually identifiable information) reported by entities (health plans and clinicians)

**Editorial page 1424**  
covered under the Health Insurance Portability and Accountability Act (HIPAA).<sup>3</sup> Under the Health Information Technology for Economic and Clinical Health Act of 2009, breaches involving the acquisition, access, use, or disclosure of protected

health information and thus posing a significant risk to affected individuals must be reported.<sup>4</sup>

When data breaches affect 500 individuals or more, the report must include the name and state of the entity breached, the number of records affected, the type and source of the breach, and the involvement of any external vendor using protected health information. Examples include the theft of unsecured laptops, dissemination of data in emails, and improper disposal of patient records. Reports are made online via form templates.<sup>3</sup>

We included breaches affecting 500 individuals or more reported as occurring from 2010 through 2013, accounting for 82.1% of all reports.<sup>3</sup> We quantified the frequency and geographic locations of breaches, adjusting for 2013 population estimates from the US Census Bureau.

Based on categorical templates, we grouped breaches as occurring via theft, loss or improper disposal of data, unauthorized data access or disclosure, hacking or information technology incidents, or other and missing ( $n = 2$ ). We described

Table. Characteristics of Data Breaches of Protected Health Information Affecting at Least 500 Individuals Reported by Entities Covered by the Health Insurance Portability and Accountability Act

	Year of Data Breach				p Value <sup>a</sup>	
	Overall	2010	2011	2012		2013
Total No. of data breaches reported	949	214	236	234	265	.07
Total No. of records affected, in millions	29.0	5.1	11.6	3.4	9.0	.88
No. of data breaches affecting at least 1 million records	6	1	3	0	2	.37
Data breach by media type, No. (%) [95% CI]						
Portable electronic device or laptop	310 (32.7) [29.7-35.7]	77 (36.0) [29.8-42.7]	72 (30.5) [24.9-36.7]	78 (33.3) [27.5-40.0]	83 (31.3) [26.0-37.2]	
Desktop, email, or EMR	148 (15.6) [13.4-18.0]	32 (15.0) [10.7-20.4]	25 (10.6) [7.2-15.2]	43 (18.4) [13.9-23.9]	48 (18.1) [13.9-23.3]	.09
Paper	212 (22.3) [19.8-25.1]	50 (23.4) [18.1-30.0]	55 (23.3) [18.3-29.2]	52 (22.2) [17.3-28.0]	55 (20.8) [16.3-26.1]	
Network server	101 (10.6) [8.8-12.8]	16 (7.5) [4.6-11.9]	25 (10.6) [7.2-15.2]	29 (12.4) [8.7-17.3]	31 (11.7) [8.3-16.2]	
Other	178 (18.6) [16.4-21.4]	39 (18.2) [13.6-24.0]	59 (25.0) [19.9-31.0]	32 (13.7) [9.8-18.7]	48 (18.1) [13.9-23.3]	
Data breach category, No. (%) [95% CI]						
Theft	552 (58.2) [55.0-61.3]	139 (65.0) [58.3-71.1]	142 (60.2) [53.7-66.3]	141 (60.3) [53.8-66.4]	130 (49.1) [43.0-55.1]	
Loss or improper disposal	105 (11.1) [9.2-13.2]	24 (11.2) [7.6-16.2]	21 (8.9) [5.9-13.3]	28 (12.0) [8.4-16.8]	32 (12.1) [8.6-16.6]	
Unauthorized access or disclosure	140 (14.8) [12.6-17.2]	16 (7.3) [4.6-11.9]	39 (16.5) [12.3-21.9]	36 (15.4) [11.3-20.6]	49 (18.5) [14.2-23.7]	.003
Hacking or IT incident	67 (7.1) [5.6-8.9]	10 (4.7) [2.5-8.5]	20 (8.5) [5.5-12.8]	14 (6.0) [3.6-9.9]	23 (8.7) [5.8-12.8]	
Other	85 (9.0) [7.3-11.0]	25 (11.7) [8.0-16.8]	14 (5.9) [3.5-9.8]	15 (6.4) [3.9-10.4]	31 (11.7) [8.3-16.2]	
Data breach involved external vendor, No. (%) [95% CI]	273 (28.8) [25.9-31.7]	54 (25.2) [19.8-31.5]	76 (32.2) [26.5-38.5]	70 (29.9) [24.4-36.1]	73 (27.6) [22.5-33.3]	.39

Abbreviations: EMR, electronic medical record; IT, information technology.

<sup>a</sup> Calculated using linear regression or  $\chi^2$  tests.

## RESEARCH LETTER

### Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017

Protections for private patient data and mandatory public reporting of breaches of data confidentiality were established by the 1999 Health Insurance Portability and Accountability Act (HIPAA) and 2009 Health Information Technology for Economic and Clinical Health Act. Between 2010 and 2013, data breaches involving at least 29.1 million patient records were reported. The ongoing transition to electronic health records may increase such breaches.<sup>1,2</sup> We used public data to examine the nature and extent of breaches from 2010 through 2017.

**Methods** | We downloaded all breaches posted to the US Health and Human Services Office for Civil Rights breach database portal between January 1, 2010, and December 31, 2017, and analyzed sector trends in number of breaches and number of records affected in terms of 3 categories reported in the federal database: *business associate*, *health plan*, and *health care provider* (terms used in the federal database); we also examined breached media and type of breach, which are defined in the figure legends.<sup>3</sup> An additional category, *health care clearing house*, had only 4 breaches and was omitted for clarity. When a breach was reported as involving multiple media or types, we attributed the full breach to each category. As such, if a single breach of 500 records involved email, laptop, and network server, then each of these 3 categories was assigned a breach of 500 records. This allowed correct reporting of breaches within each medium and breach type category but precluded summation over categories (covered entities are not multiply assigned).

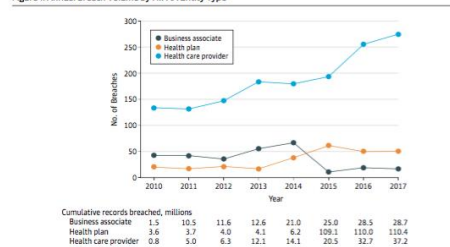
**Results** | We included 2149 breaches comprising a total of 176.4 million records. Individual breaches ranged in size from 500 to 78.8 million records. The distribution of records breached was positively skewed with a median breach affecting 2300 records (interquartile range, 995-7800) and a mean of 84 456. With the exception of 2015, the number of breach reports increased each year, from 199 in 2010 to 344 in 2017.

The most common entity breached was a health care provider, with 1503 breaches (70%) compromising a total of 37.1 million records (21%). The 278 breaches (13%) of health plans accounted for the largest share of breached records, 110.4 million (63%). Figure 1 illustrates an increasing number of breaches associated with health care providers over time.

The most common information media breached between 2010 and 2017 was paper or film, with 510 breaches (24%) comprising a total of 3.4 million records (2%; Figure 2A). However, the 410 breaches (19%) of information from network servers accounted for the largest share of breached records, 139.9 million (79%). The most commonly breached media locations shifted from laptop and paper or films in 2010 to network server and email in 2017. These shifts were paralleled by increases in hacking or information technology (IT) incidents and unauthorized access (Figure 2B), which both surpassed theft by 2016. There were 253 of 2106 breaches reported as involving multiple media (12.0%) and 83 of 2103 (3.9%) reported as involving multiple types.

**Discussion** | Despite the ethical and legal obligation to protect patient privacy and efforts to establish best practices for health care information security, breach rates have increased and health care providers accounted for a large share of those breaches.<sup>2,4-8</sup> Health plans, however, accounted for a larger

Figure 1. Annual Breach Volume by HIPAA Entity Type



	2010	2011	2012	2013	2014	2015	2016	2017
Cumulative records breached, millions	1.5	10.5	11.6	12.6	21.0	25.0	28.5	28.7
Business associate	3.6	3.7	4.0	4.1	6.2	109.1	110.0	110.4
Health plan	0.8	5.0	6.3	12.1	14.1	20.5	32.7	37.2

The numbers below each year refer to cumulative number of records breached up to that year. Business associate refers to entities that do not provide or reimburse health care but are given access to Health Insurance Portability and Accountability Act (HIPAA)-protected data, generally to support physicians or health plans. Broadly speaking, a health care provider is a person or organization who furnishes, bills, or is paid for health care service; a health plan provides, or pays the cost of, medical care (US Code of Federal Regulations 501.503). The 4 breaches of a health care clearing house were omitted for clarity.



