DRAFT

Health Care Data Breaches

An Assessment of Breach Trends in Maryland and the Nation

2010–2019

MARYLAND HEALTH CARE COMMISSION

January 16, 2020

Why Report on Breach Activity?

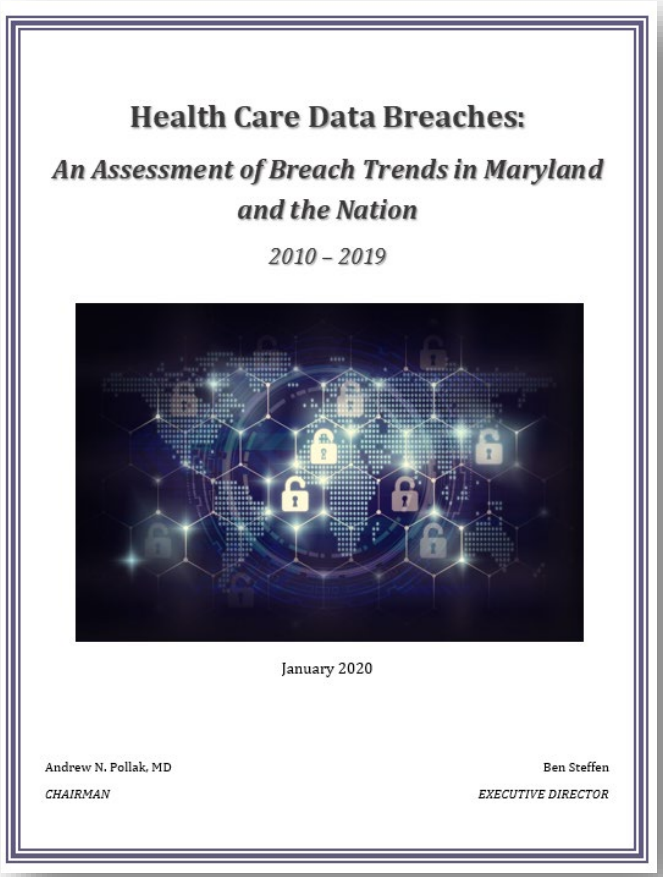
- Consistent with MHCC's Strategic Priority, Elevate Telehealth
- Awareness of breach type, frequency, and records compromised provides a framework to develop education and awareness strategies for ensuring privacy and security of protected health information (PHI)
- Aligns with MHCC's legislative charge to promote adoption of health information technology
- Support stakeholders in using the analysis to improve cybersecurity

Background

- The HIPAA Breach Notification Rule requires covered entities (CE) and their business associates (BA) to report breaches of unsecured PHI to the U.S. Department of Health and Human Services, Office for Civil Rights (OCR)
    - A breach is defined as the unauthorized acquisition, access, use, or disclosure of unsecured PHI in violation of the HIPAA Privacy Rule
- Breach notification aims to increase public transparency and accountability among CEs and BAs
    - Monetary enforcement may result if there is non-compliance, including inadequate privacy and security controls or untimely reporting

About the Assessment

- Analysis of health care data breaches affecting ≥500 individuals reported by CEs and BAs from January 1, 2010 through October 18, 2019
- Data obtained from the OCR online portal
  - Nation: N = 2,887
  - Maryland: N = 60



A Snapshot of Breaches in 2019

- Reported breach occurrences continue to rise in Maryland and the nation
- Number of breach occurrences reported in Maryland (11) represents about three percent of the national total (384)
- Estimated number of records compromised in Maryland (182K) decreased by 69 percent from the prior year compared to a 184 percent increase in records exposed nationally (39M)
- The single largest breach in the nation was a hacking/IT incident at a third-party billing collections firm exposing over 20 million records
- Hacking/IT incidents remain the most reported breach type in Maryland (since 2016) and the nation (since 2017)

Notable Findings

Breach Trends Over the Last Decade

- Proliferation of technology-related crime (i.e., cybercrime) and privilege misuse, which can go undetected for long periods of time
- Increase in reported breach occurrences
  - Nation: 177 (2010); 269 (2015); 384 (2019)
  - Maryland: 3 (2010); 8 (2015); 11 (2019)
- In 2015, breaches exposed the most records to date in the nation and Maryland (more than a six-fold increase and about a four-fold increase respectively as compared to the prior year)
  - A large majority of records compromised are attributed to a single breach resulting from a hacking/IT incident

Breach Frequency and Type

- Nationally, a health care data breach occurs almost daily (since 2017)
- Total breach occurrences reported in Maryland (60) since 2010 represents about two percent of the national total (2,887) and slightly exceeds the average among all states (55)
- Most reported breach type (2010-2019) varies in Maryland and the nation
  - Maryland: hacking/IT (45%); unauthorized access/disclosure (33%); theft (17%)
  - Nation: theft (30%); hacking/IT (29%); unauthorized access/disclosure (29%)

Records Compromised

- Total records compromised in Maryland (3M) since 2010 represents about one percent of the nation (235M) and is below the average among all states (4M)
- Hacking/IT incidents expose a large majority of records:
  - 2010-2019: Maryland (66%); Nation (77%)
  - 2015-2019: Maryland (73%); Nation (92%)
  - 2019: Maryland (89%); Nation (88%)
- Health plans are responsible for half of records compromised (2010-2019) in Maryland (49%) and the nation (50%)

Consumers Perspective

- Many consumers (70%) believe their personal information is less secure today than it was five years ago
- Attitudes regarding privacy and security vary by type of personal information

Sources
Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, 2019: www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/
RSA, *RSA Data Privacy & Security Survey 2019: The Growing Disconnect Between Consumers and Businesses*: www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf

Consumers Perspective *(Continued…)*

- Health care providers (in addition to banks) are trusted more when it comes to privacy and security compared to advertising, online retailers, social media, etc.
- Consumers are more worried about cyber-attacks that result in a breach (59%) than unauthorized access to medical devices (41%)
- Certain measures taken after a breach (safeguarding against future breaches, free credit monitoring, and timely notification) satisfy consumers more than financial compensation
- Consumers who experience a breach of their medical information (27%) are less likely to stop dealing with the responsible organization in comparison to consumers who had their credit card information exposed (37%)

Key Points

- Safeguarding PHI requires an understanding and resolution of past challenges to prepare for new and evolving cyber threats
- Lessons learned about lapses in security are the underpinnings to improve security posture and consumer trust
- Health care organizations' response to a breach is just as important as what they may or may not have done to prevent it

Appendix

Total Breach Occurrences				
Year	**Nation**		**Maryland**	
	Occurrences	*Percent Total*	*Occurrences*	*Percent Total*
2010	177	6	3	5
2011	199	7	2	3
2012	218	8	3	5
2013	276	10	4	7
2014	313	11	6	10
2015	269	9	8	13
2016	329	11	6	10
2017	353	12	8	13
2018	369	13	9	15
2019*	384	13	11	19
Total	2,887	100%	60	100%

*Note: *Data through October 18, 2019.*

Total Records Compromised				
Year	**Nation**		**Maryland**	
	Records	*Percent Total*	*Records*	*Percent Total*
2010	5,836,972	2	2,492	<1
2011	13,160,857	6	5,765	<1
2012	2,854,525	1	12,556	<1
2013	7,016,139	3	23,058	1
2014	17,451,293	7	273,719	9
2015	113,306,969	48	1,131,380	38
2016	16,659,090	7	669,919	23
2017	5,123,671	2	55,961	2
2018	13,943,464	6	589,054	20
2019*	39,647,787	17	182,416	6
Total	235,000,767	100%	2,946,320	100%

*Note: *Data through October 18, 2019.*

Breach Type 2010-2019*								
Type	**Nation**				**Maryland**			
	Occurrence	*Percent Total (Occurrence)*	*Records*	*Percent Total (Records)*	*Occurrence*	*Percent Total (Occurrence)*	*Records*	*Percent Total (Records)*
Hacking/IT Incident	823	29	180,963,637	77	27	45	1,932,586	66
Improper Disposal	88	3	1,347,863	1	-	-	-	-
Loss	185	6	8,124,594	3	2	3	1,220	<1
Other	85	3	1,339,969	1	1	2	692	<1
Theft	871	30	25,270,294	11	10	17	78,976	3
Unauthorized Access/ Disclosure	824	29	16,036,951	7	20	33	932,846	32
Unknown	11	<1	1,917,459	1	-	-	-	-
Total	2,887	100%	235,000,767	100%	60	100%	2,946,320	100%

*Notes: *Data through October 18, 2019; a strikethrough (-) signifies that no data was reported.*

Breaches by CE Type by Year						
Nation						
Year	*BA*		*Health Plan*		*Health Care Provider*	
	Occurrences	Records	Occurrences	Records	Occurrences	Records
2010	36	1,498,167	20	3,560,444	121	778,361
2011	44	8,935,715	20	90,537	134	4,133,355
2012	40	1,146,711	23	336,265	154	1,361,549
2013	64	1,058,760	18	97,555	191	5,853,320
2014	77	12,988,487	41	2,247,146	193	2,197,061
2015	14	3,992,767	61	102,919,905	194	6,394,297
2016	22	3,564,666	51	880,455	256	12,213,969
2017	21	212,754	51	347,558	281	4,563,359
2018	42	5,980,018	53	2,833,971	273	5,127,293
2019*	43	12,445,661	46	3,305,919	293	22,329,269
Total	403	51,823,706	384	116,619,755	2,090	64,951,833
Maryland						
Year	*BA*		*Health Plan*		*Health Care Provider*	
	Occurrences	Records	Occurrences	Records	Occurrences	Records
2010	1	800	1	692	1	1,000
2011	1	765	-	-	1	5,000
2012	2	2,076	-	-	1	10,480
2013	-	-	-	-	4	23,058
2014	1	10,766	3	219,620	2	43,333
2015	-	-	3	1,102,105	5	29,275
2016	-	-	-	-	6	669,919
2017	1	664	-	-	7	55,297
2018	-	-	2	20,142	7	568,912
2019*	3	57,138	1	87,400	7	37,878
Total	9	72,209	10	1,429,959	41	1,444,152

*Notes: *Data through October 18, 2019; strikethrough (-) signifies that no data was reported; breaches reported by clearinghouses or with unknown information are not included.*