ANALYSIS OF DATA BREACHES IN HEALTHCARE

(HIPAA VIOLATION)

Sanchita Ajay Gawand

MS: Information Systems

California State University Los Angeles

CIS 5250: Visual Analytics

Submitted to: Dr. Shilpa Balan

INDEX

OBJECTIVE OF STUDY

The majority of the population in the United States is covered under health insurance programs and also employer-based coverage for workers and their families. This leads to huge data in terms of confidential information about providers and patients, their medical records and entire health related history. This also extends to personal information about an individual with respect to his financial credentials. Needless to say, this data of such vital importance needs to be protected and cannot be misused. In the 1990s, it first became apparent that the medical care industry would become more efficient by computerizing medical records. A set of regulations and rules was necessary to help people carry their health insurance from one company to the next, as well as streamline the movement of medical records from one health care institution to another and also protect it. This project attempts to explore the significance of this health care law, its breaches, violations, and the data is analyzed using the Power BI tool.

DATASET

FILE FORMAT: CSV

Dataset URL's:

https://data.world/health/health-data-breaches

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

FILE FORMAT: WEB LINK

Dataset URL:

https://compliancy-group.com/hipaa-fines-directory-year/

https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-state/index.html

DATASET DESCRIPTION

This dataset contains a list of breaches of protected health information which affected more than 1000 individuals from the Year 2009 to the Year 2016. Another dataset set has a list from the Year 2017- to till date. Both the datasets have been merged for better to analyze the topic better.. Altogether, there are 2100 rows and 9 columns. Below are columns named:

1. State: Shows the state to which the breach belongs to.
2. Covered Entity: This has 3 categories: Health Plan, Healthcare, Buisiness Associate
3. Organization: This show the name of the organization
4. Business Associate Present: This column shows if business associate was present or no: Yes/No
5. Individuals Affected: This column show the number of individuals affected
6. Breach Date: This column shows the date on which breach took place
7. Breach Type: This column shows the breach types : Theft, Loss, Hacking/IT Incident, Other
8. Breach Location: This column shows where did breach took place: Desktop Computer, Loss of device, papers etc.
9. Web Description: This shows the description of the case.

Web

This dataset contains the total penalty paid by the entities each year. This has the data from the year 2015 to the year 2018. There are 5 columns and more than 100 rows.

1. Date : This column shows date when fine was charged for the breach
2. Fine Total: This column shows the fine charged for the breach

3. Organization: This column shows the organization name

4. OCR Statement Link: This column gives the organization link

5. Settlement amount: This column shows the settlement amount paid by the entities

6. Penalties charged: This column show steh penalties charged for the breached data

PHYSICAL PROPERTIES OF DATA

FieldName	Type	Sample value	Range of values	Attributes/ Format	Comments
Name of covered entity type	Textual	Brooke Army	1211 unique values, 34 duplicate	Max 21 characters	10 null, 1302 records
State	Categorical (Nominal)	CA	52 unique states	Max 12 characters	1302 records, 10 duplicates
Individuals Affected	Numerical	1000	$3000 to $9000	Whole Numbers	1302 unique records, 13 null
Breach Submission Date		10/21/09	1/1/2009 to 1/1/2018	MM/DD/YYYY	12 duplicate records, 5 null
Year	Numerical	2009	10 unique years	YYYY	Year from 2015-2018. It is been separated from breach submission date
Type of Breach	Categorical (Ordinal)	Theft	9 unique types, 3 nulls	Max 12 characters	30 null, 10 duplicates
Location of Breached Information	Categorical (Nominal)	Desktop Computer	8 unique types	Max 12 characters	1302 records, 5 null
Business	Categorical	Yes	Yes, No, 10	Max 3	1302 records, 5 duplicates

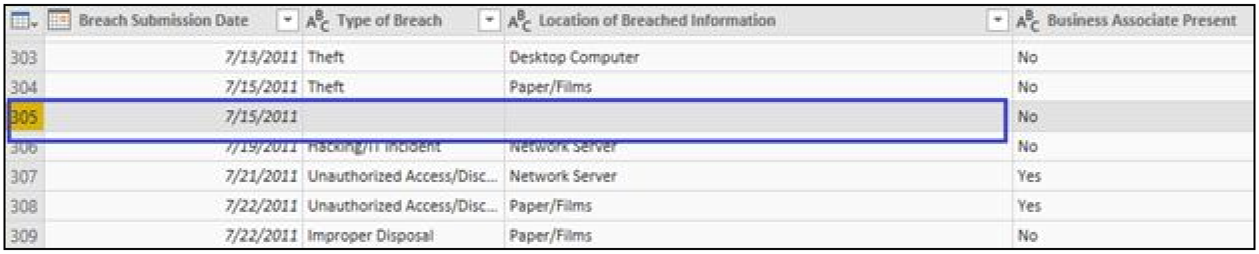
Associate Present	(Ordinal)		blank	characters	
Web Description	Textual	binder containing the protected health information (PHI) .	10 unique links	1303 unique Description	Most Descriptions are not available
Web					
State	Categorical (Nominal)	CA	52 unique states	Max 12 characters	200 records, 5 nulls
Date	Numbers	10/21/09	1/1/2009 to 1/1/2018	MM/DD/YYYY	200 records, 5 blanks
Organization		OCR	52 unique rows	Max 24 characters	200 records
Fine Total	Numbers	$1,234,567	$300000 to $12345678	Max 10 characters	10 nulls
OCR Statement Link	Textual	www.hhs.com	3 unique links	Links to Thumbnails	15 nulls
Settlement Amount	Quantitaive Ratio	$2,345,678	$300000 to $12345678	Max 10 characters	200 records

Penalties Charged	Quantitative Ratio	$4,578,979	$300000 to $12345678	Max 10 characters	200 records

DATA CLEANING:

1)Missing Values: There were lot of blank and null values. This was corrected in Power BI

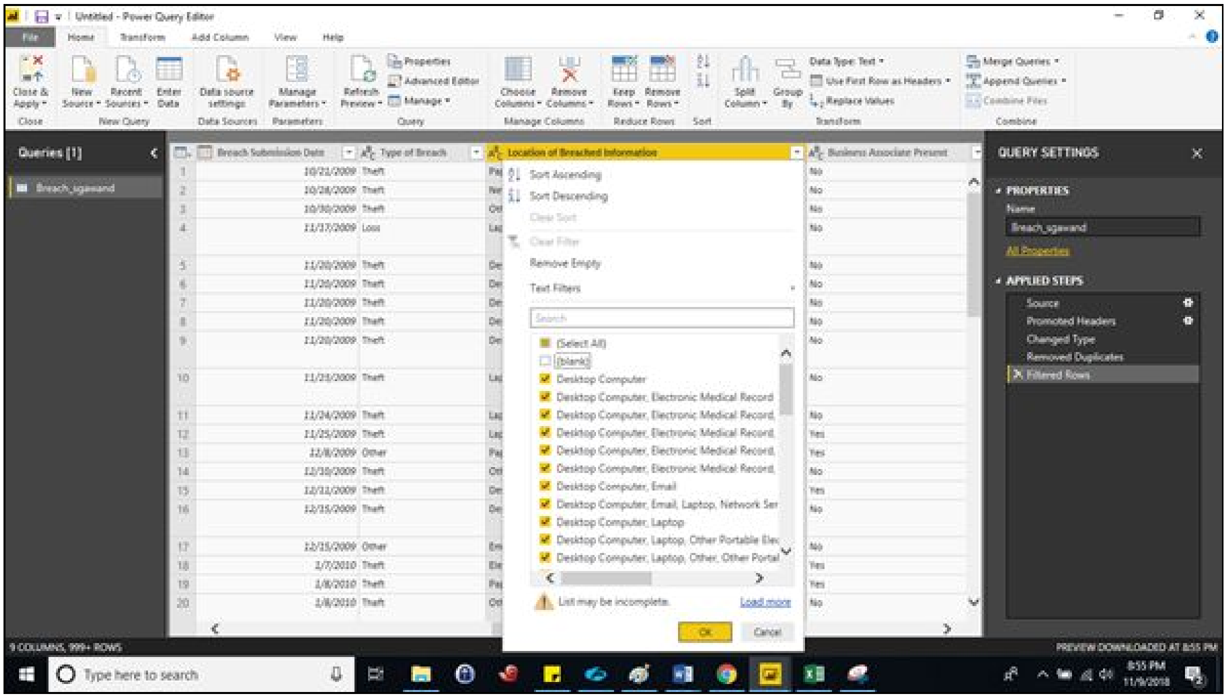
Before:



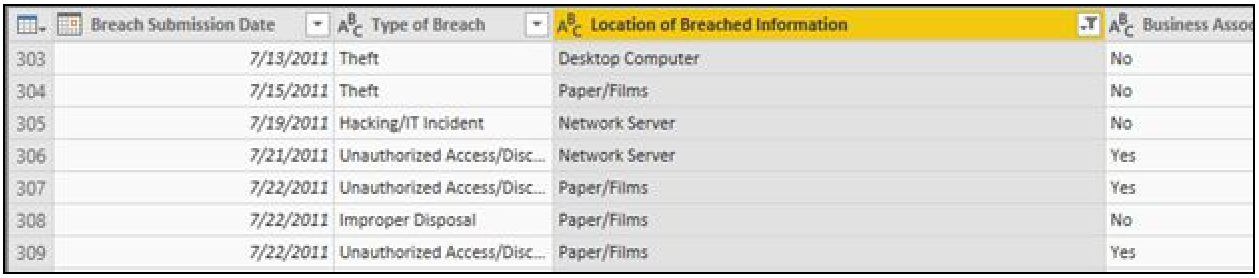
	Breach Submission Date	Type of Breach	Location of Breached Information	Business Associate Present
303	7/13/2011	Theft	Desktop Computer	No
304	7/15/2011	Theft	Paper/Films	No
305	7/15/2011			No
306	7/19/2011	Hacking/IT Incident	Network Server	No
307	7/21/2011	Unauthorized Access/Disc...	Network Server	Yes
308	7/22/2011	Unauthorized Access/Disc...	Paper/Films	Yes
309	7/22/2011	Improper Disposal	Paper/Films	No

Steps Taken:

Select Column ->Right Click -> Unselect Blank Option -> Click OK



After:

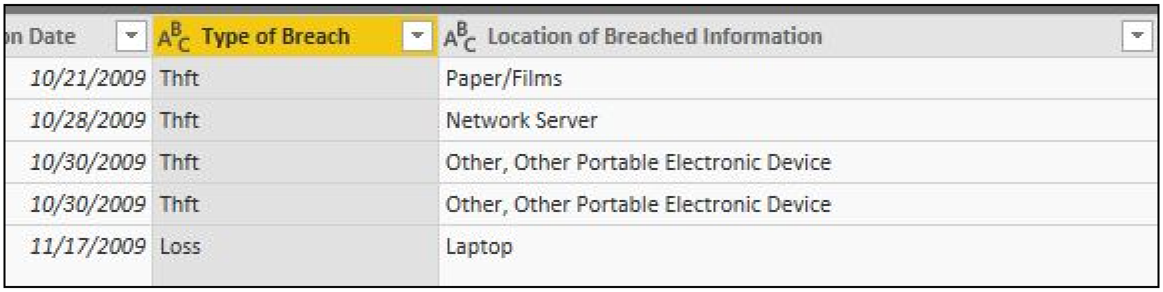


	Breach Submission Date	Type of Breach	Location of Breached Information	Business Asso
303	7/13/2011	Theft	Desktop Computer	No
304	7/15/2011	Theft	Paper/Films	No
305	7/19/2011	Hacking/IT Incident	Network Server	No
306	7/21/2011	Unauthorized Access/Disc...	Network Server	Yes
307	7/22/2011	Unauthorized Access/Disc...	Paper/Films	Yes
308	7/22/2011	Improper Disposal	Paper/Films	No
309	7/22/2011	Unauthorized Access/Disc...	Paper/Films	Yes

2) Erroneous Values

Theft was misspelled as ‘Thft’ in Type of Breach column. This was corrected in Power BI.

Before:

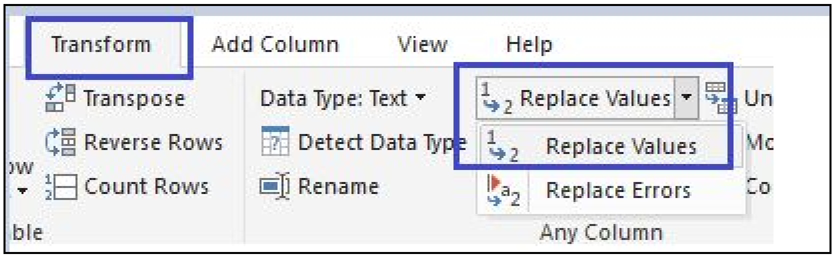


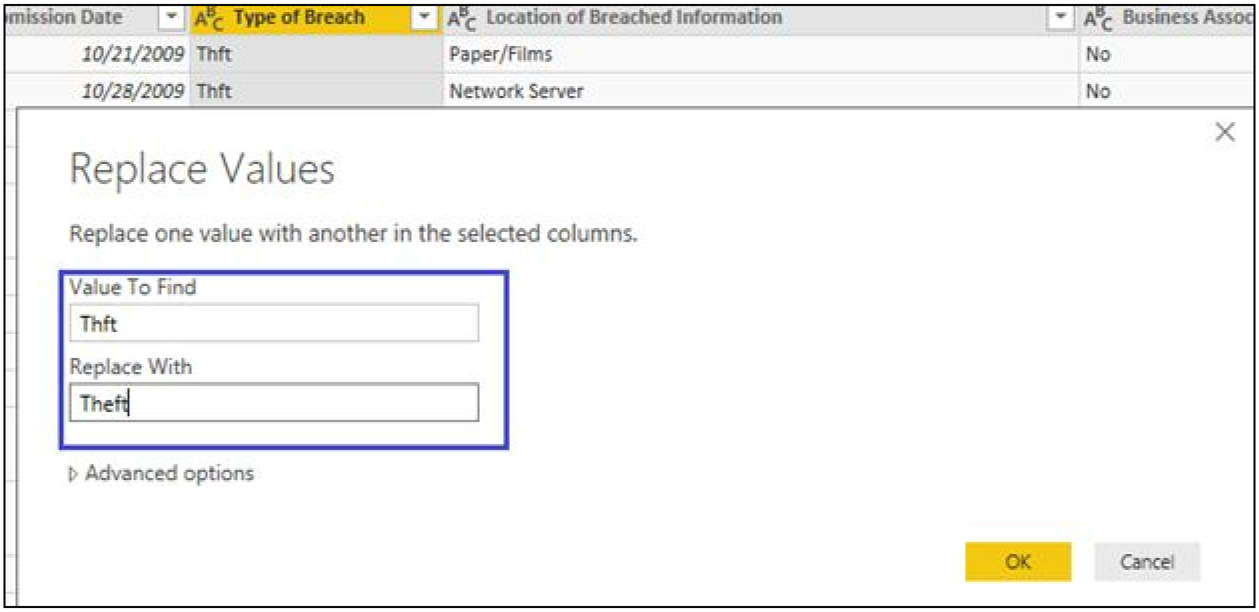
n Date	Type of Breach	Location of Breached Information
10/21/2009	Thft	Paper/Films
10/28/2009	Thft	Network Server
10/30/2009	Thft	Other, Other Portable Electronic Device
10/30/2009	Thft	Other, Other Portable Electronic Device
11/17/2009	Loss	Laptop

Steps Taken:

Select Column ->Right Click -> Transform-> Replace Values-> Insert the misspelled word **in**

Value to Find -> Insert the correct word in Replace with -> Click OK





mission Date	Type of Breach	Location of Breached Information	Business Assoc
10/21/2009	Thft	Paper/Films	No
10/28/2009	Thft	Network Server	No

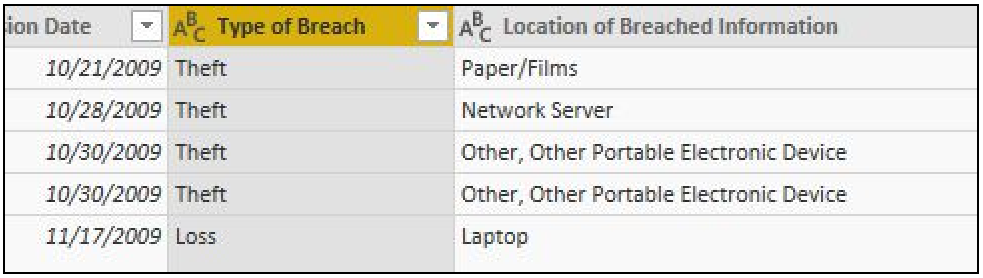
Replace Values

Replace one value with another in the selected columns.

Value To Find: Thft

Replace With: Theft

After:

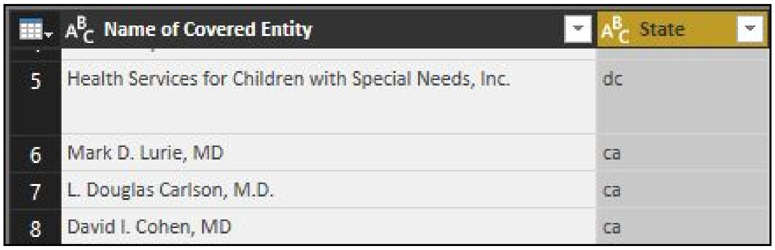


ion Date	Type of Breach	Location of Breached Information
10/21/2009	Theft	Paper/Films
10/28/2009	Theft	Network Server
10/30/2009	Theft	Other, Other Portable Electronic Device
10/30/2009	Theft	Other, Other Portable Electronic Device
11/17/2009	Loss	Laptop

3)Inconsistencies

Data inconsistencies included Changing STATE names to uppercase. This was done in PowerBI.

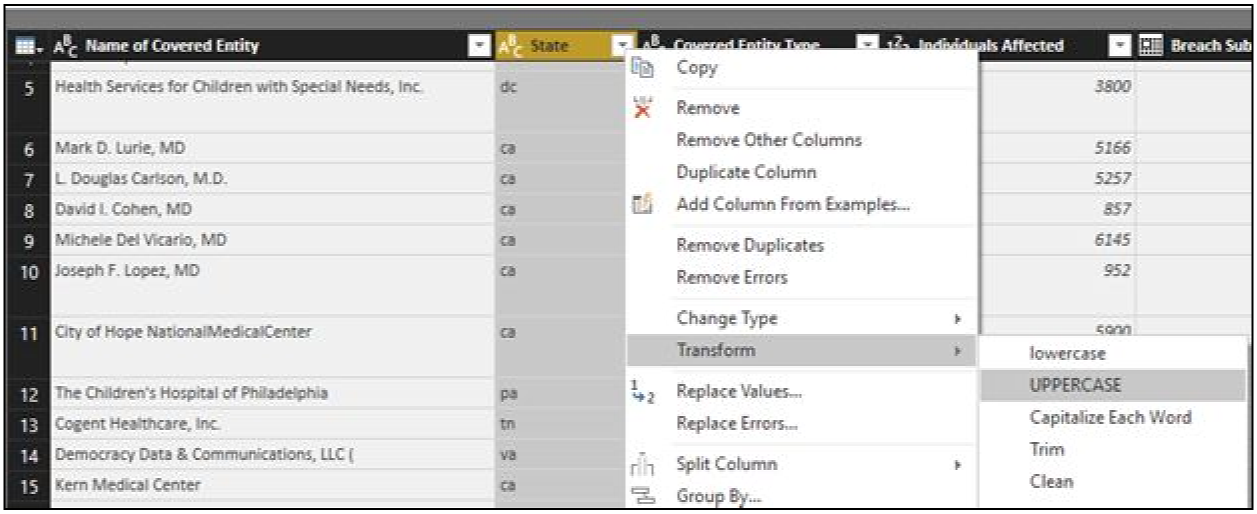
Before:



	Name of Covered Entity	State
5	Health Services for Children with Special Needs, Inc.	dc
6	Mark D. Lurie, MD	ca
7	L. Douglas Carlson, M.D.	ca
8	David I. Cohen, MD	ca

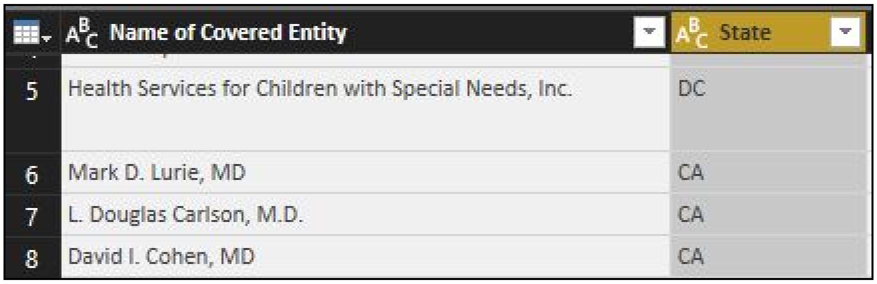
Steps Taken:

Select the column -> Right Click on column ->Transform -> Change the column to UPPERCASE.



	Name of Covered Entity	State	Individuals Affected
5	Health Services for Children with Special Needs, Inc.	dc	3800
6	Mark D. Lurie, MD	ca	5166
7	L. Douglas Carlson, M.D.	ca	5257
8	David I. Cohen, MD	ca	857
9	Michele Del Vicario, MD	ca	6145
10	Joseph F. Lopez, MD	ca	952
11	City of Hope NationalMedicalCenter	ca	5900
12	The Children's Hospital of Philadelphia	pa	
13	Cogent Healthcare, Inc.	tn	
14	Democracy Data & Communications, LLC (	va	
15	Kern Medical Center	ca	

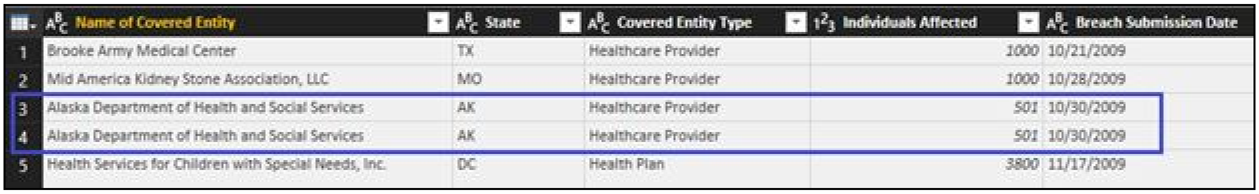
After:



	Name of Covered Entity	State
5	Health Services for Children with Special Needs, Inc.	DC
6	Mark D. Lurie, MD	CA
7	L. Douglas Carlson, M.D.	CA
8	David I. Cohen, MD	CA

4) Duplicate Records:

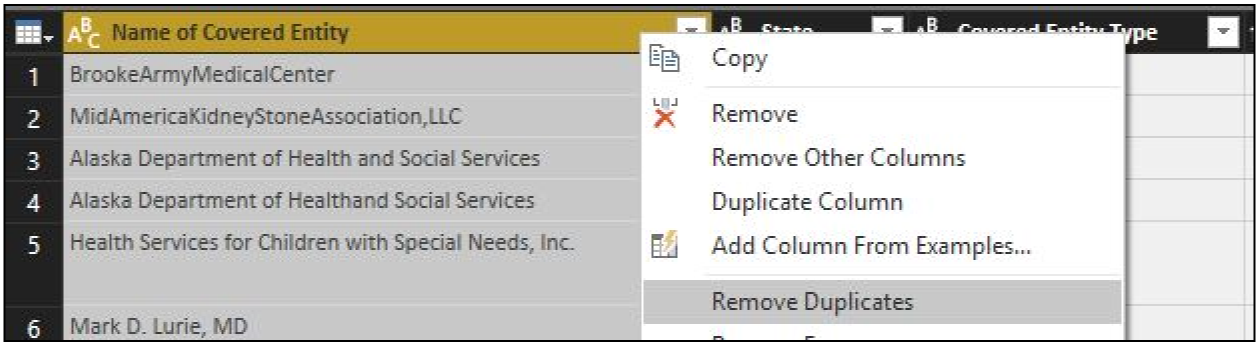
There were duplicate records found for Name of Covered Entity Type. It was removed by taking steps in PowerBI.



	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date
1	Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009
2	Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009
3	Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009
4	Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009
5	Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009

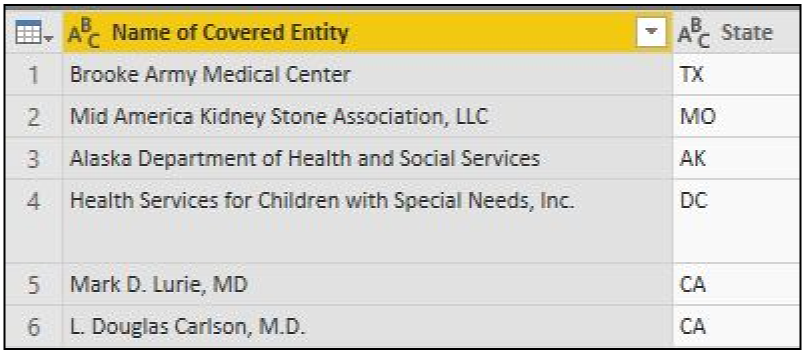
Steps Taken:

Select Column -> Right Click -> Remove Duplicates



	Name of Covered Entity
1	BrookeArmyMedicalCenter
2	MidAmericaKidneyStoneAssociation,LLC
3	Alaska Department of Health and Social Services
4	Alaska Department of Healthand Social Services
5	Health Services for Children with Special Needs, Inc.
6	Mark D. Lurie, MD

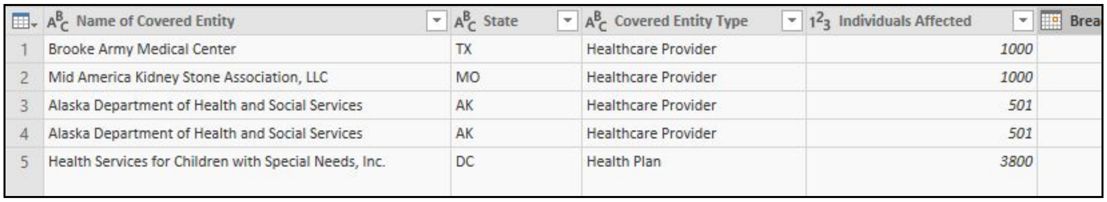
After:



	Name of Covered Entity	State
1	Brooke Army Medical Center	TX
2	Mid America Kidney Stone Association, LLC	MO
3	Alaska Department of Health and Social Services	AK
4	Health Services for Children with Special Needs, Inc.	DC
5	Mark D. Lurie, MD	CA
6	L. Douglas Carlson, M.D.	CA

5) Out of date: Values that might have expired in accuracy, like someone's age or any statistic that would be reasonably expected to have subsequently changed.

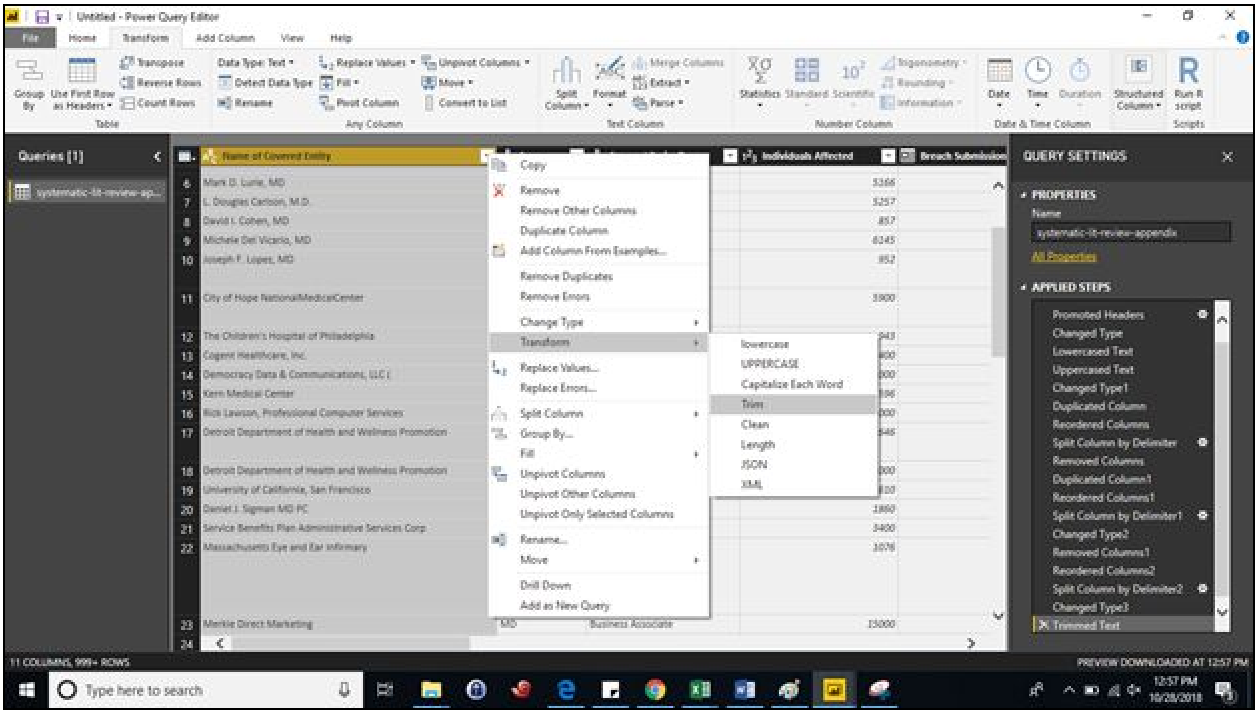
There was no such data in datasheet.



	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Brea
1	Brooke Army Medical Center	TX	Healthcare Provider	1000	
2	Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	
3	Alaska Department of Health and Social Services	AK	Healthcare Provider	501	
4	Alaska Department of Health and Social Services	AK	Healthcare Provider	501	
5	Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	

6) Leading or trailing issues: There were no leading or trailing issues found. But if they were found that could have been sorted by TRIM Option in Power BI.

It could have been corrected by -> Select column -> Transform -> Trim



	Name of Covered Entity	Individuals Affected
6	Mark D. Lurie, MD	5166
7	L. Douglas Carlson, M.D.	5257
8	David I. Cohen, MD	857
9	Michele Del Vicario, MD	6145
10	Joseph F. Lopez, MD	852
11	City of Hope NationalMedicalCenter	3900
12	The Children's Hospital of Philadelphia	
13	Cogent Healthcare, Inc.	
14	Democracy Data & Communications, LLC (	
15	Kern Medical Center	
16	Rick Lawson, Professional Computer Services	
17	Detroit Department of Health and Wellness Promotion	
18	Detroit Department of Health and Wellness Promotion	
19	University of California, San Francisco	
20	Daniel J. Sigman MD PC	1850
21	Service Benefits Plan Administrative Services Corp	3400
22	Massachusetts Eye and Ear Infirmary	1076
23	Merkle Direct Marketing	15000
24		

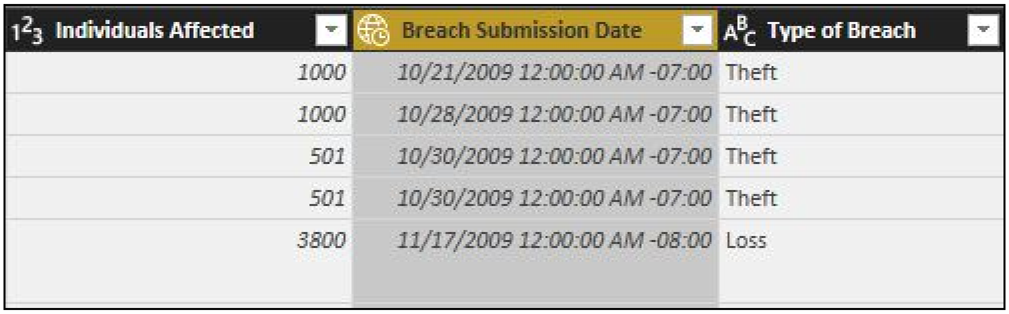
Name: systematic-lit-review-appendix

APPLIED STEPS:
Promoted Headers
Changed Type
Lowercased Text
Uppercased Text
Changed Type1
Duplicated Column
Reordered Columns
Split Column by Delimiter
Removed Columns
Duplicated Column1
Reordered Columns1
Split Column by Delimiter1
Changed Type2
Removed Columns1
Reordered Columns2
Split Column by Delimiter2
Changed Type3
Trimmed Text

7) Date Format:

Wanted the Date format in only date format. Didn't want to include time. Cleaned it by taking steps in Power BI.

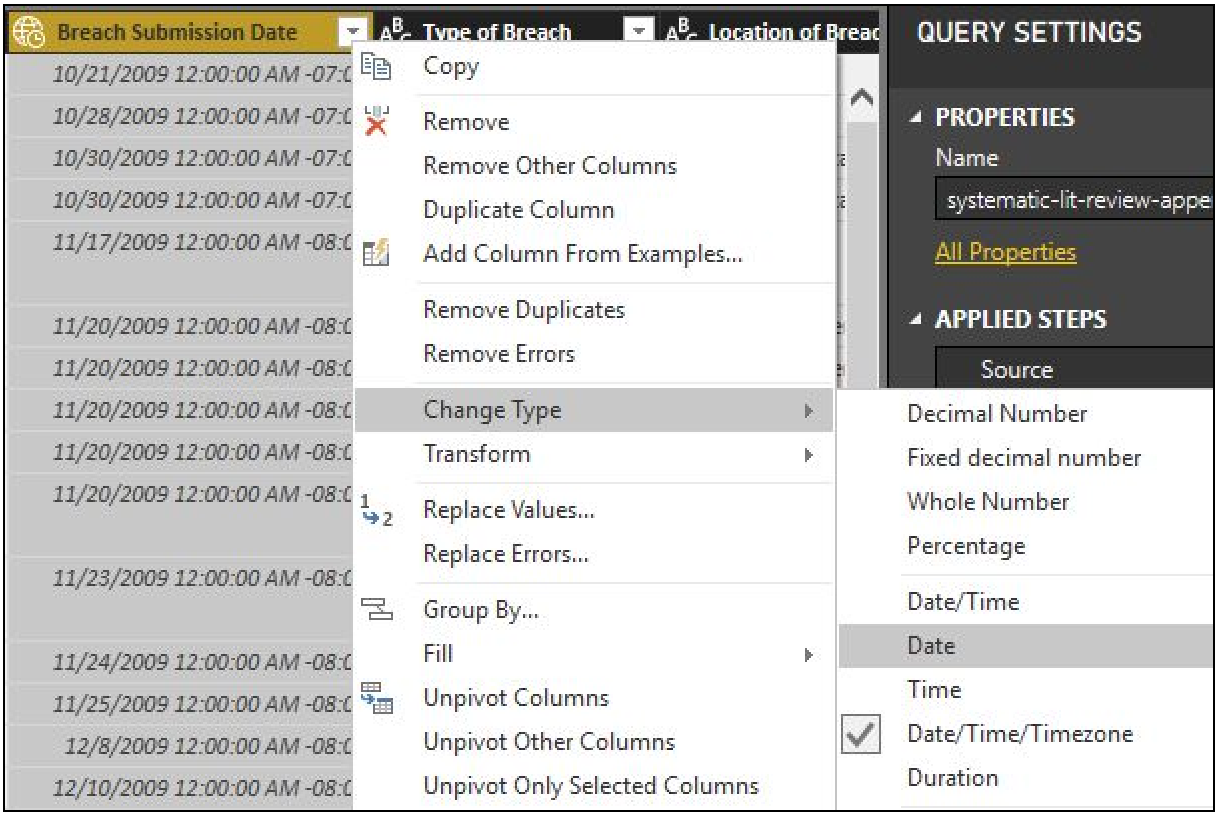
Before:



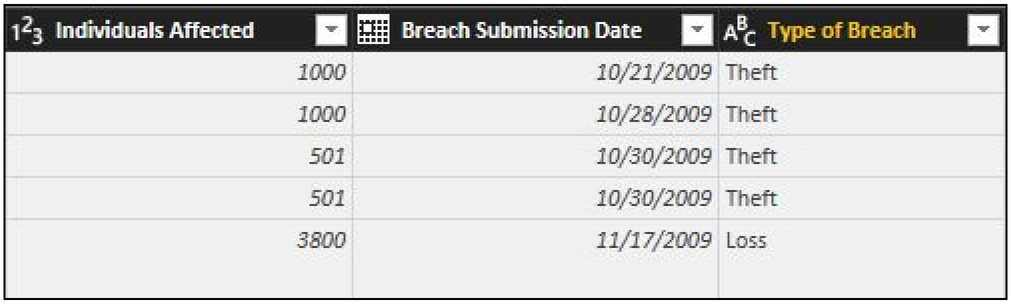
Individuals Affected	Breach Submission Date	Type of Breach
1000	10/21/2009 12:00:00 AM -07:00	Theft
1000	10/28/2009 12:00:00 AM -07:00	Theft
501	10/30/2009 12:00:00 AM -07:00	Theft
501	10/30/2009 12:00:00 AM -07:00	Theft
3800	11/17/2009 12:00:00 AM -08:00	Loss

Steps Taken:

Select Column -> Right Click -> Change Type -> Date


Breach Submission Date
Type of Breach
Location of Breac
QUERY SETTINGS
10/21/2009 12:00:00 AM -07:(
10/28/2009 12:00:00 AM -07:(
10/30/2009 12:00:00 AM -07:(
10/30/2009 12:00:00 AM -07:(
11/17/2009 12:00:00 AM -08:(
11/20/2009 12:00:00 AM -08:(
11/20/2009 12:00:00 AM -08:(
11/20/2009 12:00:00 AM -08:(
11/20/2009 12:00:00 AM -08:(
11/20/2009 12:00:00 AM -08:(
11/23/2009 12:00:00 AM -08:(
11/24/2009 12:00:00 AM -08:(
11/25/2009 12:00:00 AM -08:(
12/8/2009 12:00:00 AM -08:(
12/10/2009 12:00:00 AM -08:(
Copy
Remove
Remove Other Columns
Duplicate Column
Add Column From Examples...
Remove Duplicates
Remove Errors
Change Type
Transform
Replace Values...
Replace Errors...
Group By...
Fill
Unpivot Columns
Unpivot Other Columns
Unpivot Only Selected Columns
PROPERTIES
Name
systematic-lit-review-appe
All Properties
APPLIED STEPS
Source
Decimal Number
Fixed decimal number
Whole Number
Percentage
Date/Time
Date
Time
Date/Time/Timezone
Duration

AFTER

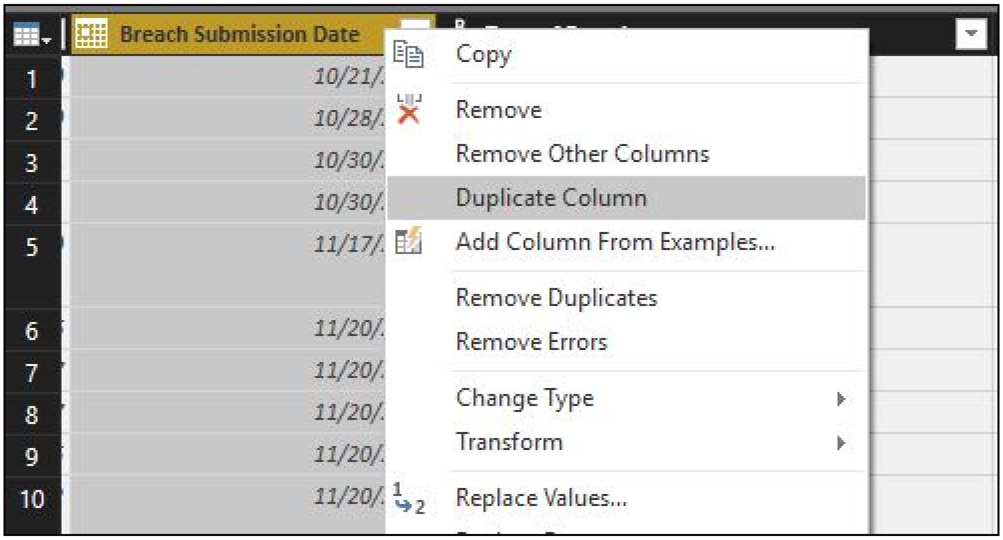


Individuals Affected	Breach Submission Date	Type of Breach
1000	10/21/2009	Theft
1000	10/28/2009	Theft
501	10/30/2009	Theft
501	10/30/2009	Theft
3800	11/17/2009	Loss

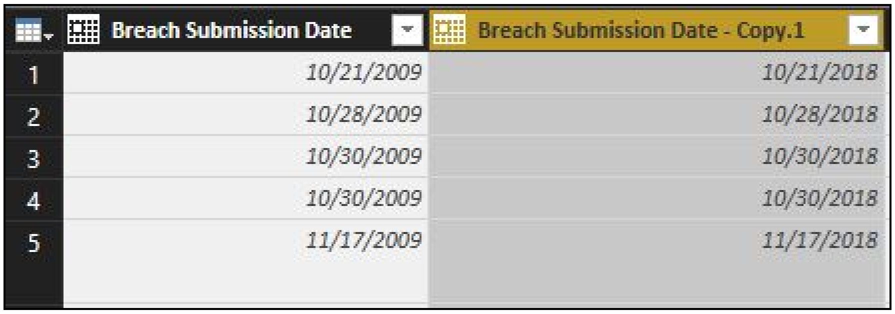
8) Other Data Types:

Splitting into Year column: Before and Steps Taken: Splitted month, year and day in different columns

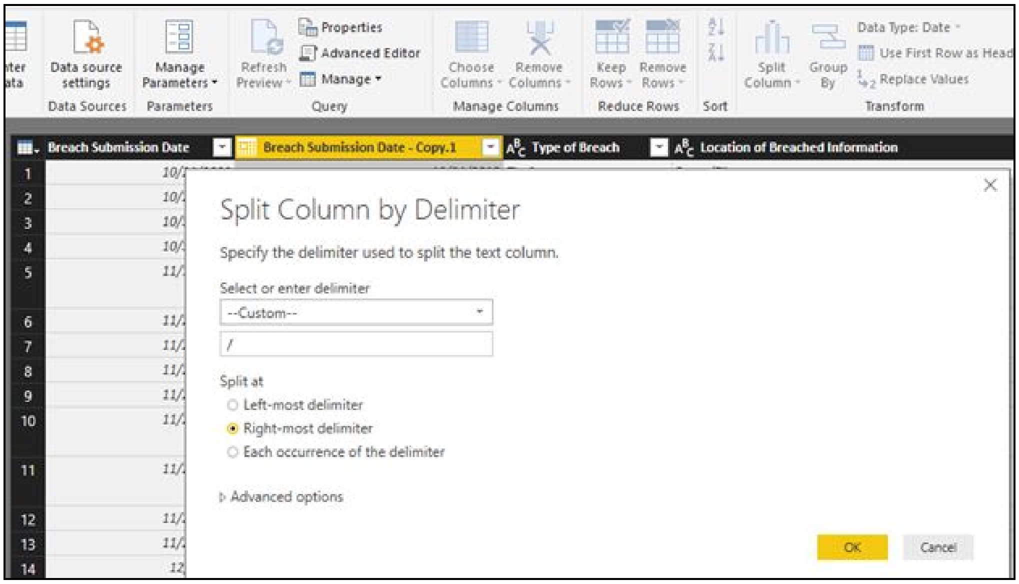
Select column ->Duplicate Column-> split by delimeter



	Breach Submission Date
1	10/21/.
2	10/28/.
3	10/30/.
4	10/30/.
5	11/17/.
6	11/20/.
7	11/20/.
8	11/20/.
9	11/20/.
10	11/20/.



	Breach Submission Date	Breach Submission Date - Copy.1
1	10/21/2009	10/21/2018
2	10/28/2009	10/28/2018
3	10/30/2009	10/30/2018
4	10/30/2009	10/30/2018
5	11/17/2009	11/17/2018



Split Column by Delimiter

Specify the delimiter used to split the text column.

Select or enter delimiter

--Custom--

/

Split at

○ Left-most delimiter

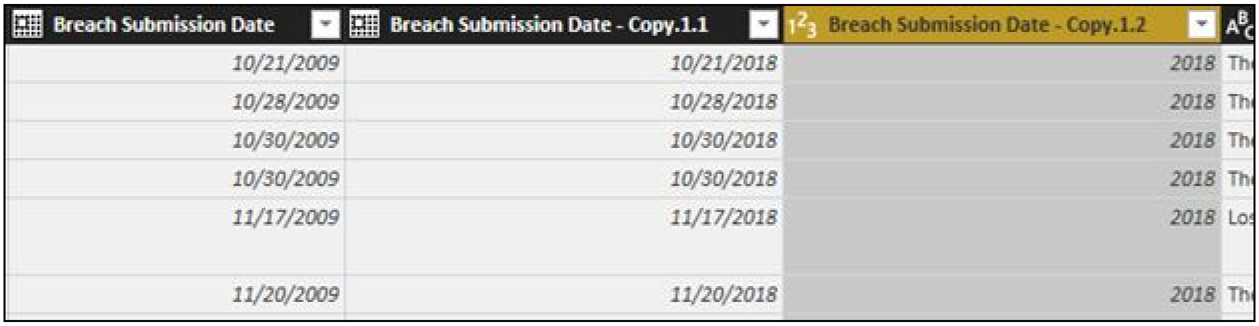
● Right-most delimiter

○ Each occurrence of the delimiter

Advanced options

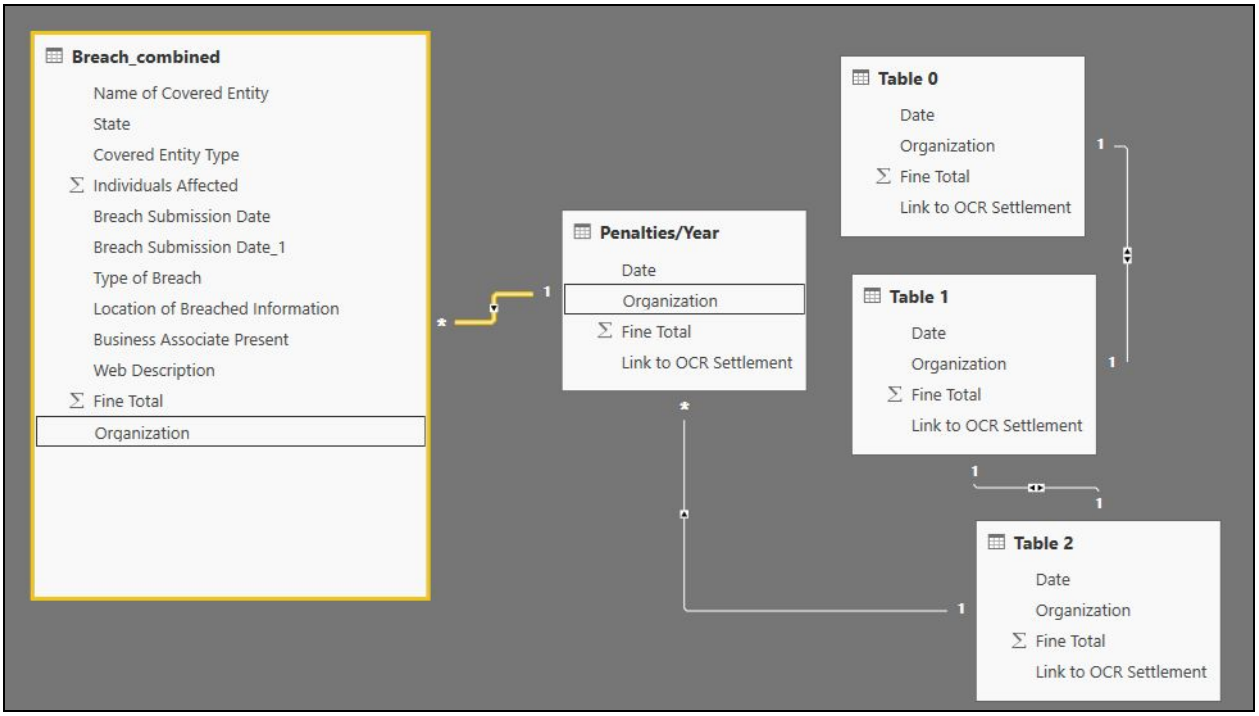
OK Cancel

After :



Breach Submission Date	Breach Submission Date - Copy.1.1	Breach Submission Date - Copy.1.2	
10/21/2009	10/21/2018	2018	Th
10/28/2009	10/28/2018	2018	Th
10/30/2009	10/30/2018	2018	Th
10/30/2009	10/30/2018	2018	Th
11/17/2009	11/17/2018	2018	Lo
11/20/2009	11/20/2018	2018	Th

RELATIONSHIP BETWEEN TABLES:



Primary Key: Organization

Foreign Key: Penalty

Cardinality: One to One (1:1) - This means the column in one table has only one instance of a particular value, and the other related table has only one instance of a particular value.

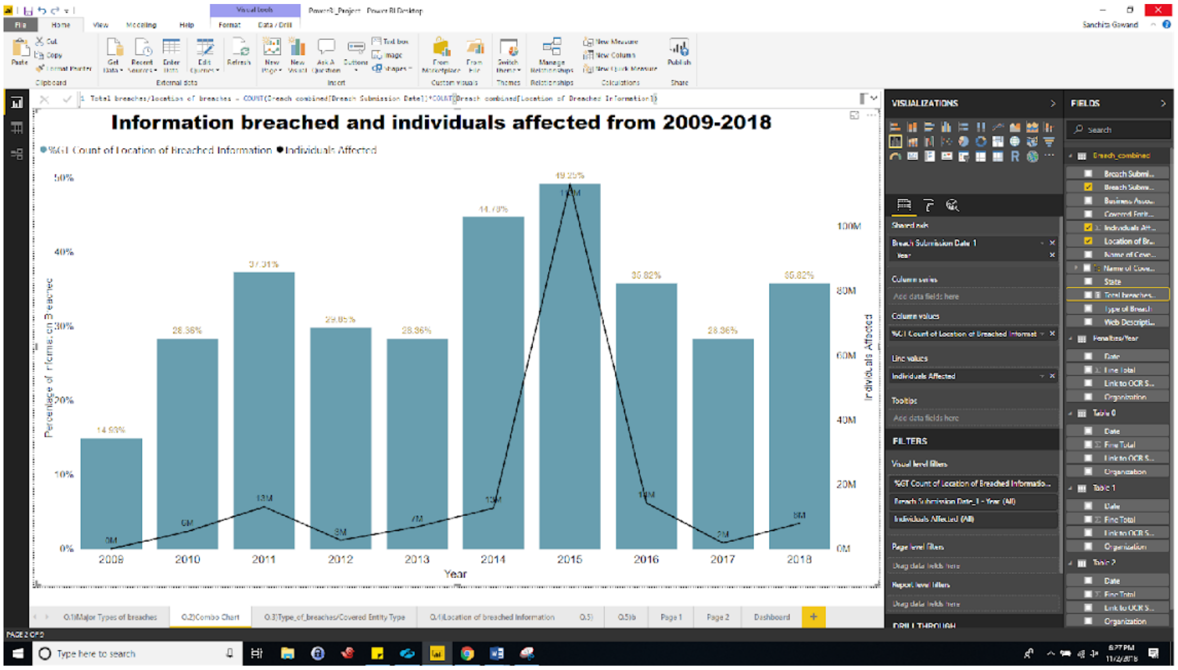
This relation is created as it will help to analyse how much penaties is paid by each organization individually yearly and in total. This will help to understand the overall penalty till now paid due to violation of HIPPA

MEASURE USED:

Total breaches/location of breaches measure was created to show the count of all the breaches with respect to individuals affected each year.

Formula:

Total breaches/location of breaches = COUNT(Breach_combined[Breach Submission Date])*COUNT(Breach_combined[Location of Breached Information])



```
1 Total breaches/location of breaches = COUNT(Breach combined[Breach Submission Date])*COUNT(Breach combined[Location of Breached Information])
```

Information breached and individuals affected from 2009-2018

Shared axis: Breach Submission Date 1, Year

Column series: Add data fields here

Column values: %GT Count of Location of Breached Informat

Line values: Individuals Affected

Tooltips: Add data fields here

Visual level filters: %GT Count of Location of Breached Informatio...; Breach Submission Date_1 - Year (All); Individuals Affected (All)

Page level filters: Drag data fields here

Report level filters: Drag data fields here

VISUALS AND DASHBOARD

QUESTIONS: VISUALS

Q.1) Show the top 4 major types of breaches?

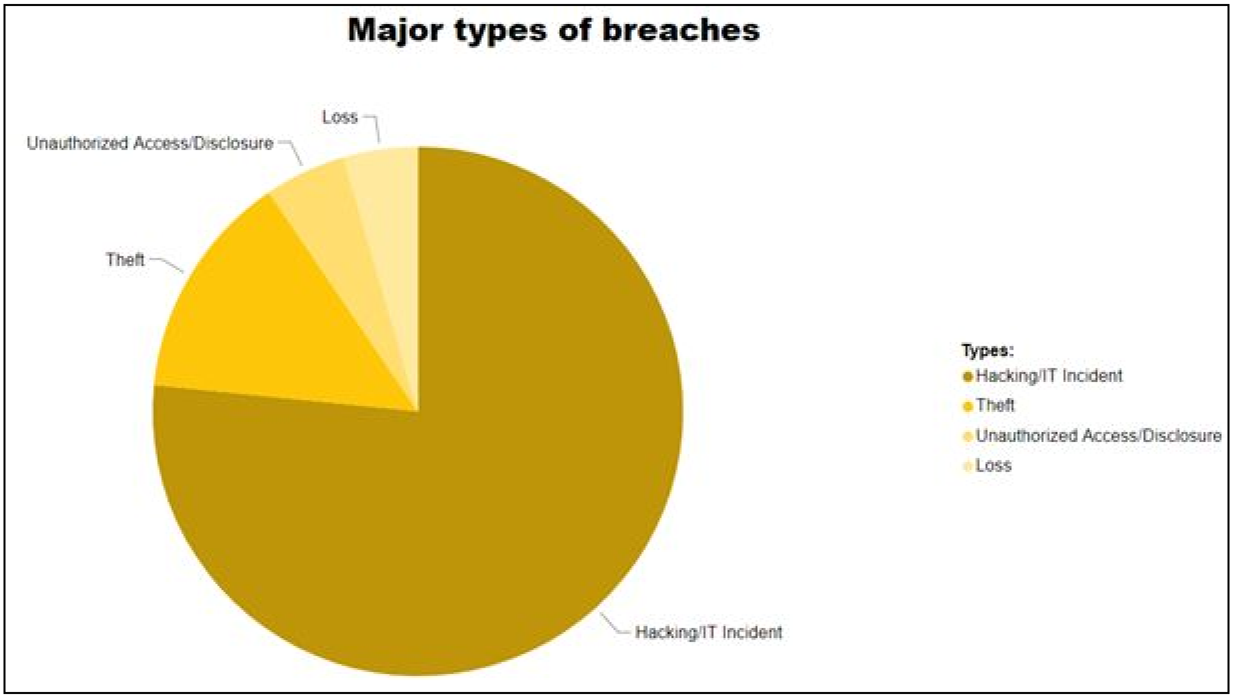


Chart Type: Pie Chart

Filtered by Top 4, Data colors, Legends, Labels

This visual shows major types of breaches which have taken place in healthcare and affected the majority of individuals. As shown in the above visual, top four majority breaches are due to Hacking/IT Incident, theft, unauthorized access/disclosure and loss. Maximum breaches are due to Hacking/IT Incident i.e 76%. This includes for example a person intentionally gains unauthorized access to a system or device. Nearly half of incidents attributed to hacking involve the use of stolen credentials. For eg; two employees of the Minnesota Department of Human Services fell for phishing attacks, which potentially breached 21,000 patient records over the course of more than one month in July 2018. As shown above, 13.92% are due to Theft. Other two are Unauthorized Access/Disclosure ie 4.96% and Loss (4.54%).

Q.2) Show the individual affected by types of breach and covered Entity Type?

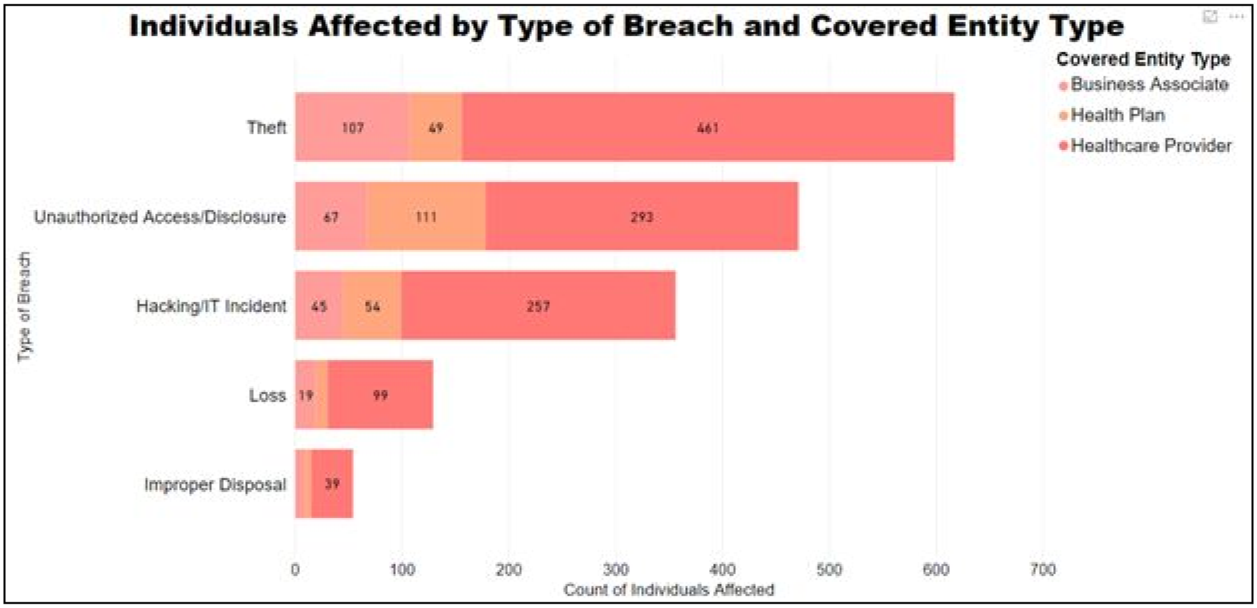


Chart Type: Stacked Bar

Filter, Data Color, Labels, Legend

This visual shows the individuals affected by the type of breach and covered Entity type. X-Axis shows the count of individuals affected and Y-axis show Type of breaches. Highest Type of Breach is Theft and least is due to Improper Disposal. Five types of breaches are shown above: Theft, Unauthorized access/disclosure, Hacking/IT Incident, Loss, Improper Disposal. Each breach is grouped according to 3 covered entity type: Business Associate, Health Plan, Healthcare Provider. Highest individuals are affected due to Theft ie 461 for Healthcare Provider, 107 for Business Associate, 49 individuals for Health Plan.

Q.3) Show how many individuals were affected each year wrt to the information breached on Desktop Computer, Electronic Medical Record and Email?

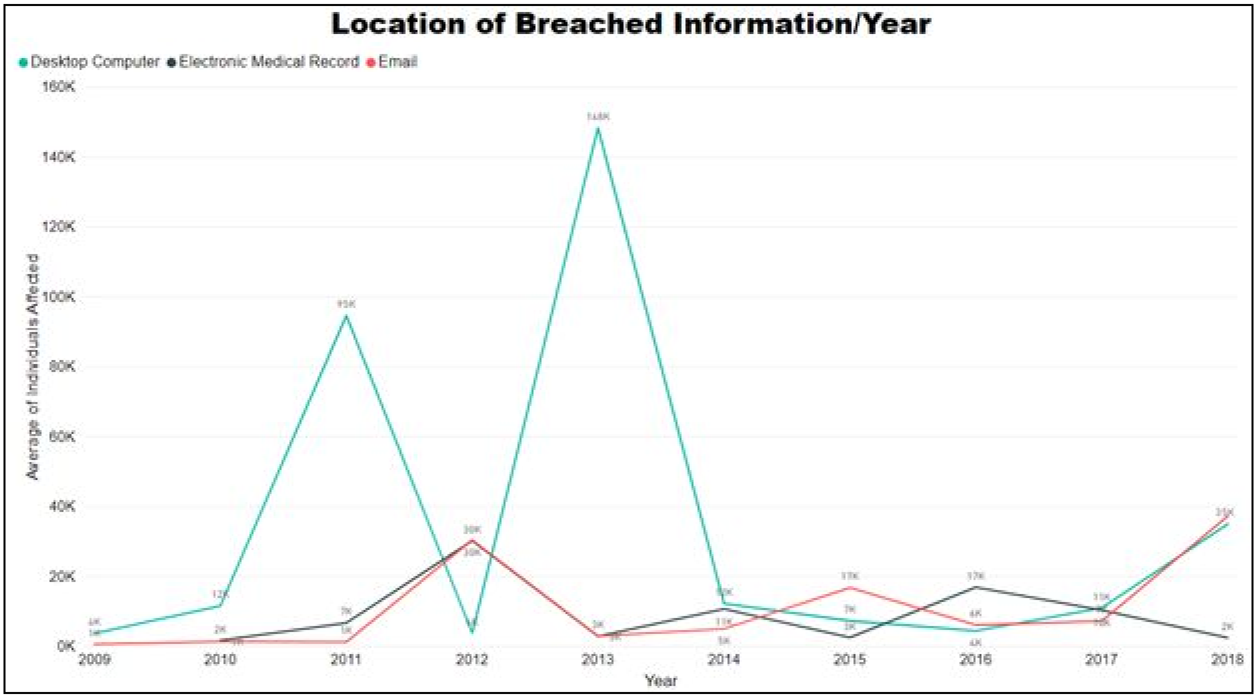


Chart Type: Line Chart

Filter, Data Label, Data Color, Data Labels

Line chart shows the series of value changed over temporal plane. This visual shows count of individuals affected by the location of breach each year from 2009 to 2015. The x-axis represents Year and Y-axis represents the Average number of individuals affected. Three breached location represented are Desktop Computer, Electronic Medical Record and Email. Highest number of desktop breaches took place in year 2013 which affected on an average 140 k individuals. Also as shown, majority of breaches due to email and electronic medical record took place in year 2012 which affected around 20k individuals. As per the visualization, highest breaches takes place on desktop computer.

Q.4)Show overall information breached and individuals affected from 2009 to 2018?

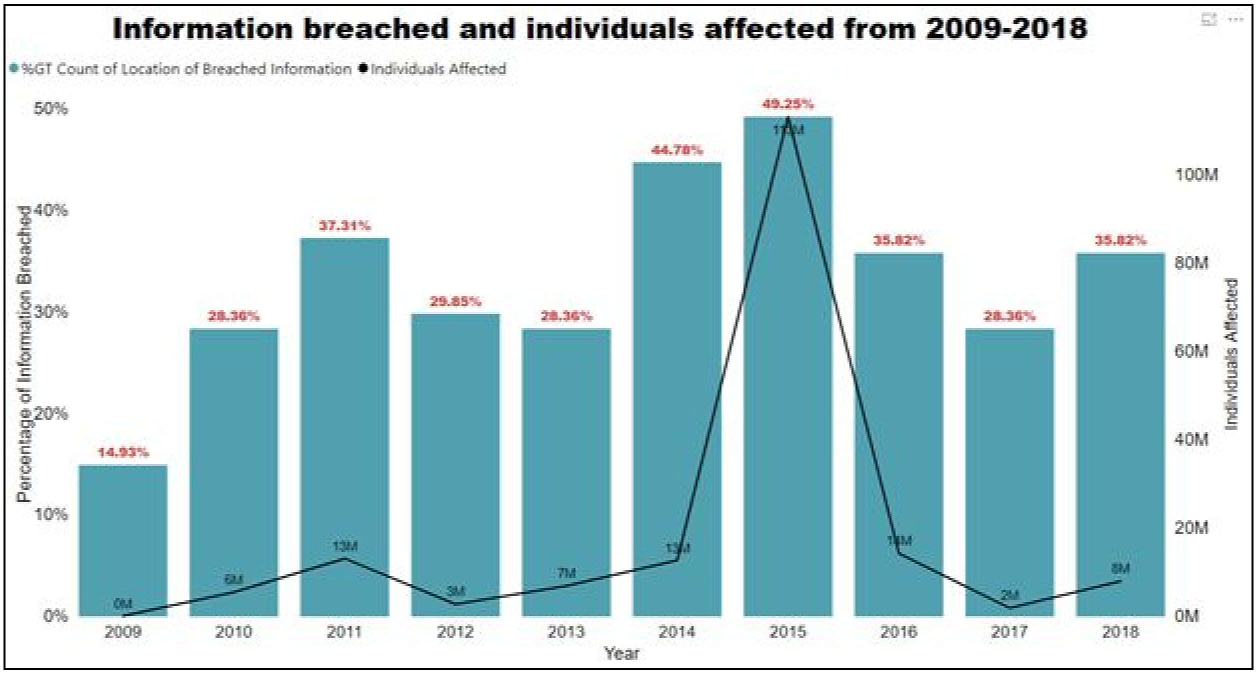


Chart Type: Combo Chart

Dual Axis, Data Label, Data Colors, Percentage, Filter, Measure

Above visual shows the information breached and individuals affected by 2009-2018. The x-axis represents the Year and Y-Axis represents Percentage of Information Breached. Measure has is been created to show total Total breaches/location of breaches measure was created to show the count of all the breaches with respect to individuals affected each year. As shown above, 49.25% of information was breached which affected around 113 millions of people. Least breaches which affected less individuals was in year 2009. For year 2018 around 35 % of information has been breached.

Q.5) How much fine was paid due to a violation of HIPPA Policy each year?

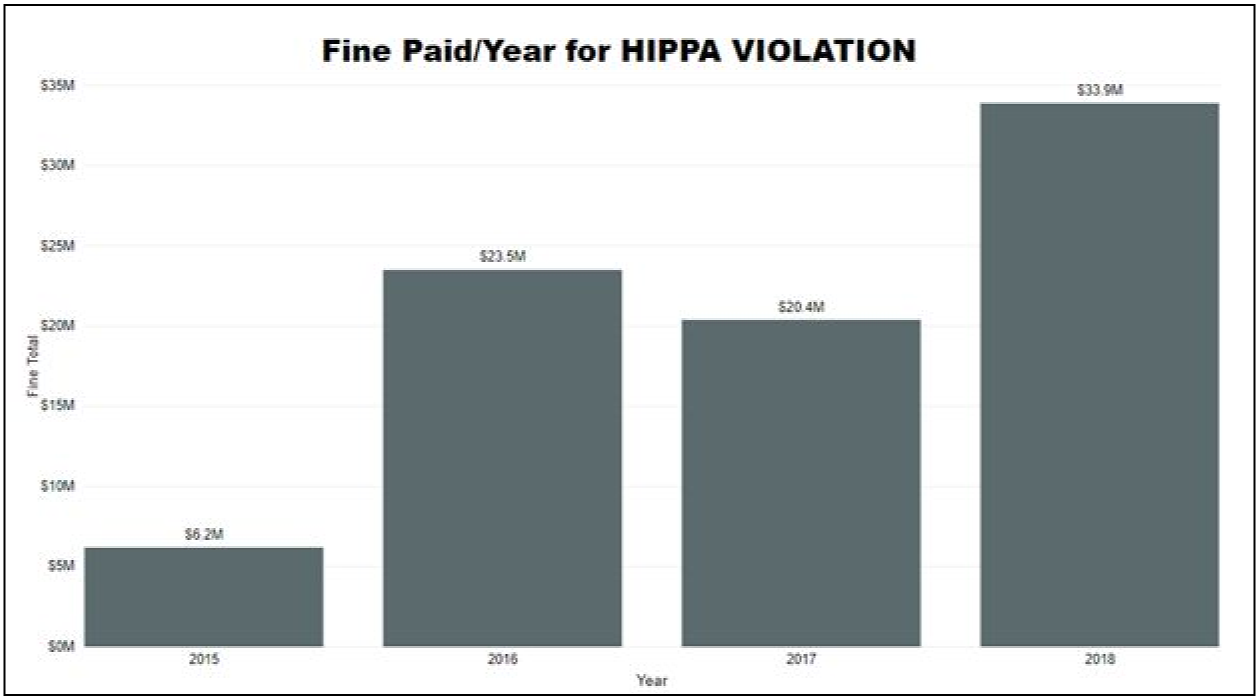


Chart Type: Bar Chart

Filter, Data Labels, Data Colors

Above visual shows, the fine paid each year for data breach i.e HIPAA Violation. X-Axis represents Year and Y-Axis represents Penalty Charges paid each year. Majority of penalty was paid in 2018 ie $33.9 M. In Year 2015, $6.2 M was paid for the data breached.

Q.6) Show the Fine Total Paid till date?

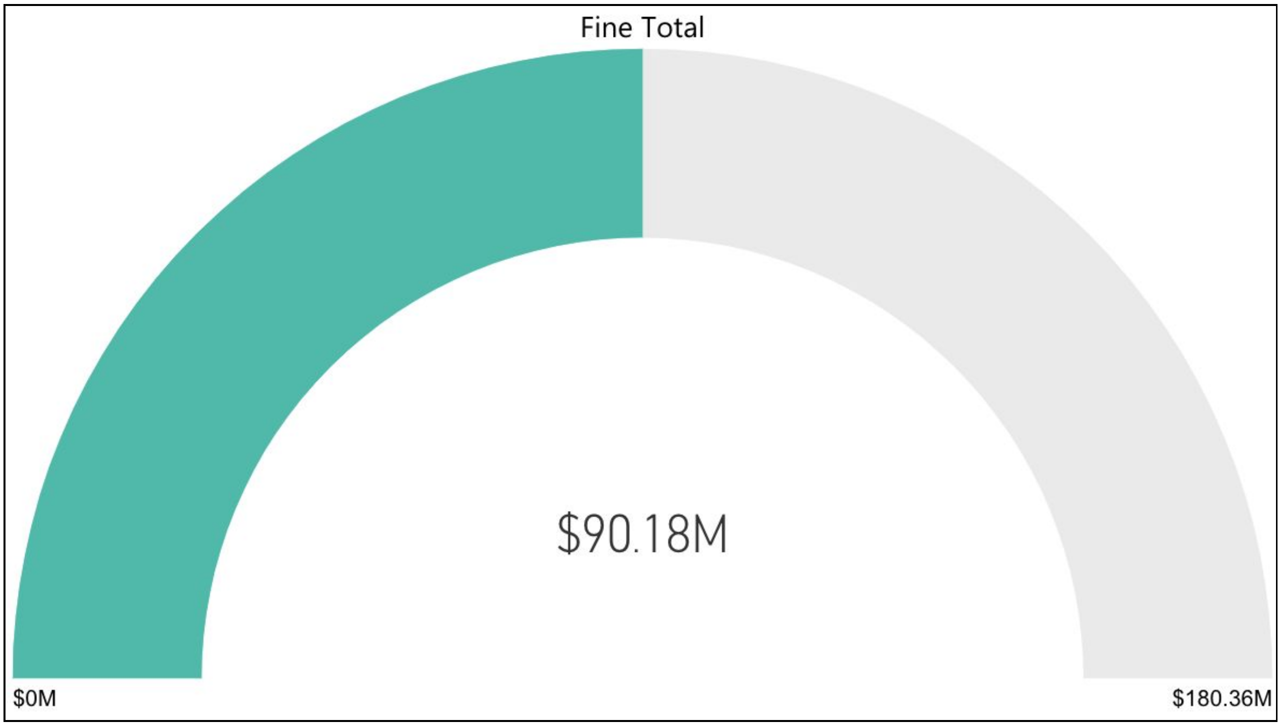
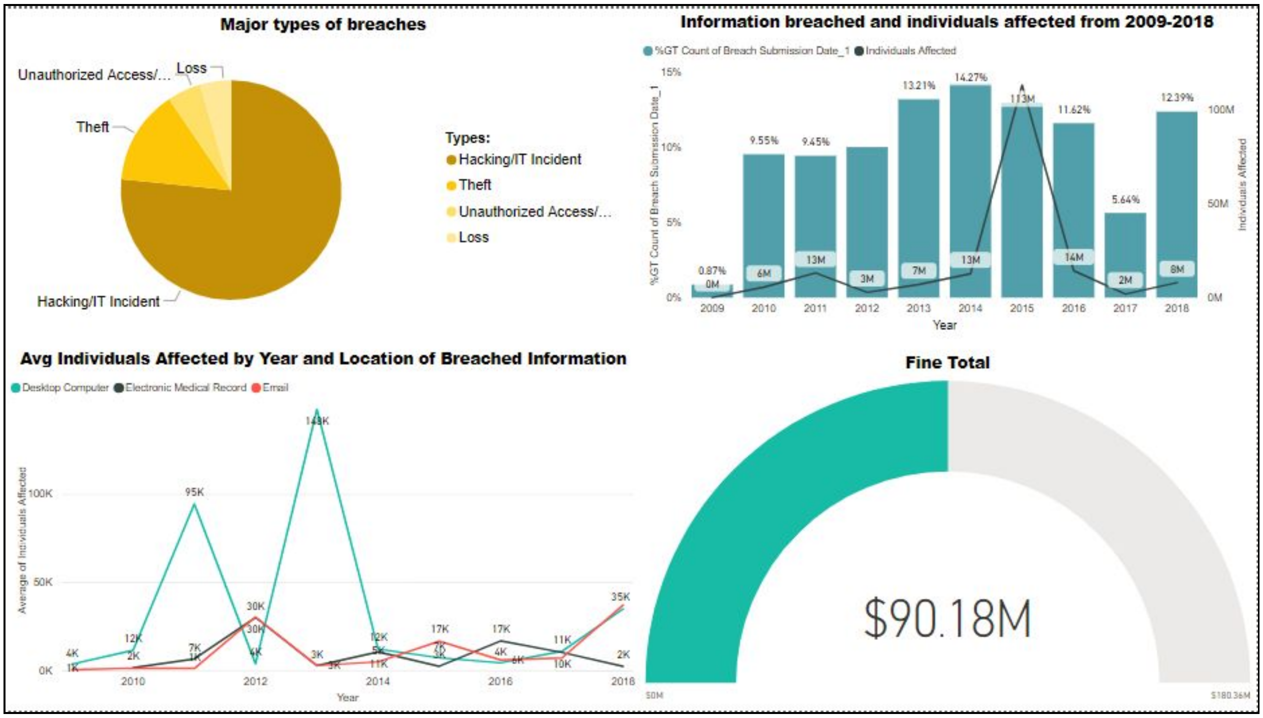


Chart Type: Gauge Chart

Filter, Data Labels, Data Colors

Above visualization show the total penalty paid till date ie $90.18M due to Data breaches. This shows how much loss it is.

DASHBOARD:



Above Fig shows the dashboard for the visualizations created. This dashboard helps us to analyze what type of breaches take place, where does most breaches takes places, how much individuals affected each year and how much penalty is paid till date.

STORYTELLING:

Summary of data breaches in hospital industry have become common nowadays especially in the healthcare industry. As per the visualizations and the data studied more that 5678900 of individuals are affected due to data breaches in healthcare till date from 2009.

To start with, major types of breaches which occur more often in healthcare is due to Hacking/IT Incident, followed by Theft, Unauthorized access and loss of devices. Study shows of breaches which comprises of more that 132923498 of individuals affected till date. As per our Study, hacking incidents is the type of breach which is the major breach (75.23 %). Hacking incidents occur when a person intentionally gains unauthorized access to a system or device. The most common technique is for hackers is to steal access credentials. 70.5% of the security incidents are an account of malware incidents according to the report.

Further followed by theft and unauthorized access breaches. Many practices may focus on infrastructure when preparing their information security policies for Health Insurance Portability and Accountability Act (HIPAA) audits, but a new study has shown that the majority of data breaches are the result of theft. The study showed that 68 percent of security breaches were due to the loss or theft of mobile devices or files. Further, 48 percent of data lost was on a laptop, desktop computer or mobile device. Employees accessing patient information when they are not authorized is another very common HIPAA violation. Whether it is out of curiosity, spite, or as a favor for a relative or friend, this is illegal and can cost a practice substantially. Misuse of PHI or selling that information could lead to fines or imprisonments. In 2016 unintended disclosure was the major reason for the incidents with malware on the second rank. The same fashion followed in 2015 as well, but there was not as far of a gap, as approximately one-third of incidents stemmed from unintended disclosure and about 27 percent were caused by hacking or malware. Theft of PHI (protected health information) through lost or stolen laptops, desktops, smartphones, and other devices that contain patient information can result in HIPAA fines. Mobile devices are the most vulnerable to theft because of their size; therefore, the necessary safeguards should be put into place such as password protected authorization and encryption to access patient-specific information. On Nov. 5, 2012, the U.S. Department of Health and Human Services Office for Civil Rights received notification from Women & Infants Hospital of Rhode Island that unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals, were missing. The tapes held protected health information, including patient name, date of birth, date of exam, physician names, and, in some instances, Social Security Numbers.

Location of Breaches: Desktop computer, Electronic Medical Record, Email

Desktop: Highest during year 2013 ie 1.4 k average individuals were affected. (Give example how this breach can take place) For example The theft of a laptop computer containing information of nearly 1,400 patients was among two HIPAA breaches that led a Pennsylvania provider of remote heart monitoring to pay $2.5 million.

Electronic Medical Record: Highest during 2012 : average 30k individuals affected (give example how this breach takes a=place and how it can affect the patients and overall)

Emails: highest during 2018. Avg 35 k individuals affected. (Give example how this can happen and how it affects upto which rate to any individual)

An example which includes this unintended data disclosure, such as emails containing PHI sent to the wrong recipient or servers left publicly accessible, accounted for 41 percent of reported health data breaches the first nine months in 2017, according to research from Beazley. In Dec

2015, Mary Ruth Buchness, a dermatologist practicing in New York City, accidentally emailed a list of nearly 15,000 patient names and corresponding addresses, appointment dates and Social Security numbers.

Individuals affected Each Year

In the year 2014: 14.27 % of breaches took place which affected more than 100 millions people. According to a survey conducted by Health Information Privacy/Security Alert of data released by the HHS Office for Civil Rights (OCR) approximately 174,792,250 people have been affected by 1,996 HITECH breaches through July 17, 2018.

In approximately 409 breaches business associates were involved with 31,239,362 patients potentially exposed. Among the 1,996 breaches, the main cause of breach is theft has been laptop theft resulting in over 5.5 million individuals impacted. But it has been seen that the major reason for breaches and leaks has been hacking of servers. With over 119 million patients affected in the past 6 months, IT incidents still rank the top. As of June 30, Office of Civil Rights (OCR) had received 158,834 complaints with the 2017 monthly average of around 2,000.

Penalties charged

A prime way to avoid HIPAA violations is to educate the staff and people dealing with it and spread awareness of the existing and new reforms. People should be aware about the degree of penalties they and the organizations would face for any violations. Organize constant trainings to in workplace to educate people and to answer any questions they might have. Conduct HIPAA training on the softwares and educating people of revisions and updates is very important. It is very crucial to invest time and resources to ensure that your organization HIPAA compliant.

One of the main reasons for HIPAA violations is loss or theft of mobile phones and smart devices are storing patient information. The covered entities and business associates are obligated to make sure that their devices are secure and safe all the time and make sure they are not a subject to get stolen or lost. It is necessary to not only maintain this carefulness for yourself but it is important to continually remind employees and colleagues of the safety of their devices.

A great way to ensure that your device is protected is to enable two factor authentication, firewalls , encryption and secure communication on your mobile devices. In case of a loss or theft that can trigger a remote lock or erase of data from the mobile. This is a good fail safe to ensure that the data is not breached even after the phone is stollen. Also not only these devices need to be equipped with such software but also need to be periodically updated. The difficulty and complication levels must be very hard. It is very necessary to have this protocols to be put into place by the employers to make sure that they continue to be HIPAA compliant and the data is secure.

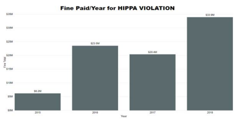
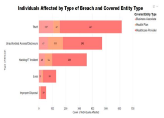
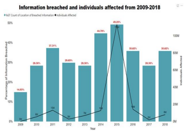
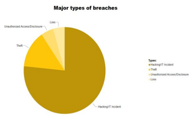
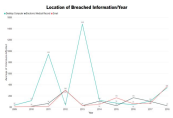
It is very important to handle physical paper data and electronic data very carefully. A misplacement of this paperwork can lead to unintentional and disastrous consequences. It is natural to be distracted during work and many employees fall prey to such misfillings of paper. It is very important to remind employees to be careful who handle paperwork of patients and be very attentive in categorizing and storing the files of sensitive patient data.

It is very important to dispose and correctly shred out paper and patient data that contains PHI. On many occasions files and papers are not discarded correctly and sensitive data has been leaked because of that. Switching to a complete electronic system is the best way to avoid these problems and stay HIPAA compliant. If paper files are necessary then it is important to make sure that the process is extremely secure, careful and employees are well aware of the recuperations. Another way to stay secure and not fall prey to any breaches or loss of information is to keep sensitive data in plain view and access of visitors and patients. It needs to be kept extremely securrely and out of reach of unauthorized people.

Lastly, it is important for employees to responsibly use their social media accounts and ensure that they do not leak any sensitive information.It has become a platform where they chances of leaking any information and it leading to a HIPAA violation has tremendously increased. It is very important to not post any information, pictures, audio, video or anything that could relate to a HIPAA violation even on a professional or personal blog.

Ultimately for the organization to be HIPAA compliant the employees need to be HIPAA compliant. Everyone must be well educated of the rules and regulations and must be aware of the sensitive information and consequences of HIPAA breaches.

PURPOSE MAP

Analysis/ Tone		Explanatory		Exhibitory	Exploratory	
		Sequence|Drama	annotate|describe	display	Manipulate|interrogate	Participate|contribute
Reading	Utilitration|efficient|precision	 Fig.1		 Fig.3		 Fig.4
Feeling	emotive|seductive|big-picture		 Fig.2	 Fig.5		

Purpose Map helps to plot your expectation of what will be the best-fit type of solution to facilitate the desired purpose. It offers a high-level view of landscape shaped by different relationships across dimensions. Horizontal dimension of this map concerns the experience of the visualization. Along this spectrum there are three states against which you define your intentions: **Explanatory, Exhibitory and Exploratory.**

Tones: The vertical dimension of the purpose map concerns the intended tone of the visualization, with reading tone positioned on the top and feeling tone positioned on the bottom. Reading Tone would be best-fit approach when the purpose of your work requires you to facilitate understanding with high degree of precision and detail.

Feeling Tone is the best fit when the data cannot be readed it just can be felt

Explanatory: Explanatory visualizations are found on the left side of the map. It provides the viewer with a visual portrayal of subject's data and will also take some responsibility to bring key insights to the surface, rather than leave the prospect of interpreting the meaning of the information entirely to the viewer.

As shown, Fig.1 explains how much penalties were paid each year and it falls in the reading tone where the viewer can take key insights rather than interpreting.Fig. 2 which shows the major types of breaches also gives the detailed description to the viewer. It follows the feeling tone where it gives the big picture about the breaches.

Exhibitory: In this visualization viewers have to do the work to interpret meaning, relying on their own capacity to make sense of the display of data and the context of subject-matter. Exhibitory projects rely entirely on and make assumptions about the capacity of and interest among the target audience. As shown in Fig.3 and Fig 5. which shows the individuals affected by type of breaches and covered entity type and year respectively where viewers have to make their assumptions and falls in reading as well as feeling tone as it shows the big picture.

Exploratory: In this user find their own sights. The task of interpreting and comprehending will largely be the responsibility will largely be the responsibility of viewer to form. In this viewer explores different measures concerning the dimension changes of wood, over time, across selected cities of the world. It is intended as an exhibitor experience- As Fig.5 visual display of this data- that lets you as a user draw your own conclusions, find your own shapes of interest, and look up the year that you want to see data for.

REFERENCES

1. Jacqueline Biscobing. “What Is HIPAA (Health Insurance Portability and Accountability Act)? - Definition from WhatIs.com.” *SearchHealthIT*, Margaret Rouse, July 2017**,** **https://searchhealthit.techtarget.com/definition/HIPAA**
2. Compliancy Group. “What Is HIPAA Compliance? | HIPAA Requirements.” *Compliancy Group*, Compliancy Group, 4 July 2018, **https://www.google.com/url?q=https://compliancy-group.com/hipaa/&sa=D&ust=1537654008686000&usg=AFQjCNHULGZG7TFL0GXKFVhsVBlmo_f7oA**
3. Good, Travis. “HIPAA and Data Breaches.” *The Datica Academy*, Datica Health, Inc., 14 Apr. 2016, **https://www.google.com/url?q=https://datica.com/academy/hipaa-and-data-breaches/&sa=D&ust=1537654008690000&usg=AFQjCNFyHvGoBMZIOBZaenMyckSkGoKvDQ**
4. *HIPAA Journal*, HIPAA JOURNAL, 26 Mar. 2018, **www.hipaajournal.com/civil-penalty-for-knowingly-violating-hipaa**
5. *Managed Data Center News*, Thu Pham, 6 Sept. 2013, **https://www.google.com/url?q=http://resource.onlinetech.com/how-a-hipaa-breach-can-negatively-impact-your-business/&sa=D&ust=1537654008687000&usg=AFQjCNHCIsRP0ajGgjE0AokamEQLLcXnCQ**
6. Cohen, Jessica Kim. “OCR Issuing Fewer HIPAA Penalties in 2018, Report Suggests.” *Becker's Hospital Review*, 31 July 2018,

www.beckershospitalreview.com/cybersecurity/ocr-issuing-fewer-hipaa-penalties-in-2018-report-suggests.html

7. “Health Data Breaches - Dataset by Health.” *Data.world*, 10 Jan. 2017, https://data.world/health/health-data-breaches
8. “U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.” *U.S. Department of Health & Human Services - Office for Civil Rights*, May 2017, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
9. Sivilli, Frank. “HIPAA Violation & Breach Fines | List of HIPAA Violations.” *Compliancy Group*, Compliancy Group, 21 Sept. 2018, https://compliancy-group.com/hipaa-fines-directory-year/
10. “7 Ways Employees Can Help Prevent HIPAA Violations.” *HIPAA One*, 18 Mar. 2015, www.hipaaone.com/7-ways-employees-can-help-prevent-hipaa-violations/