Team F presents

Novum Medici Clinic

Legal, Privacy & Ethics in Analytics
Final Presentation

Type of Data Collected

Novum Medical Clinic

- Communication Transcript
- Official Medical Report
- Patient Record
- Prescriptions Record
- Diagnosis
- ETC

Clinic Background

●○○ Introduction

We are data scientists from Novum Medici Clinic from New York and California, who recently expanded our location to Madrid, Berlin, and Beijing. Our clinic offers both online and offline treatments as well as therapies for our patients.

●●○ Situation

As such, the amount of our patients who're visiting our multi-locations have increased significantly in the last 2 years.

●●● Problem

However, due to several regulations/laws placed in each jurisdiction, the clinic is challenged with patients' data privacy and data transfer.

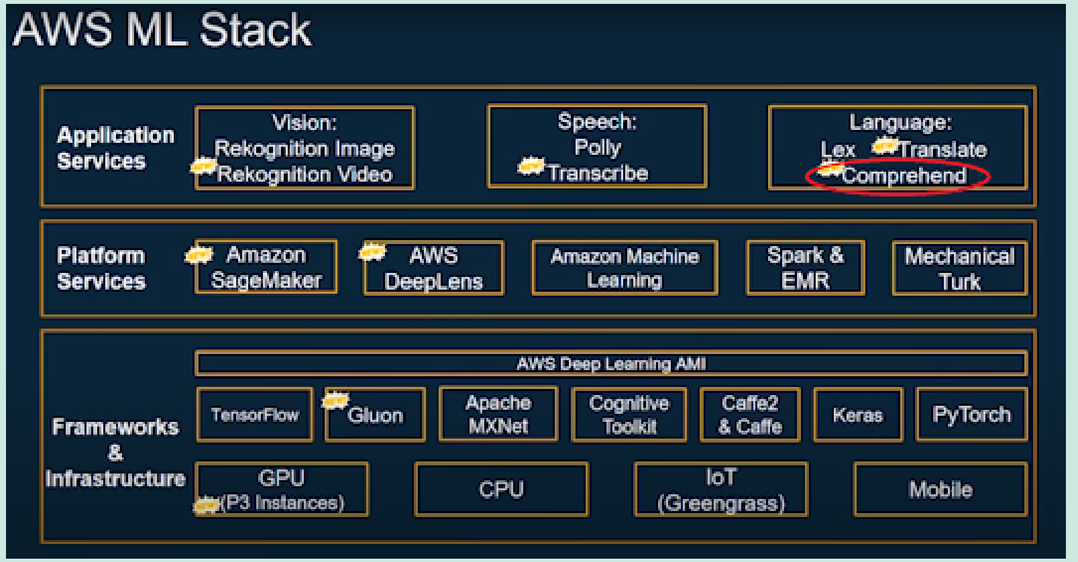
Product Description

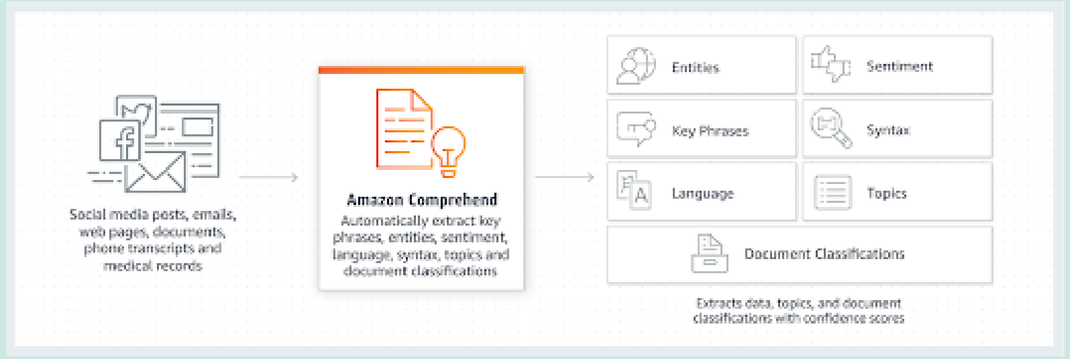
AMAZON COMPREHEND:

- *Part of the Amazon Web Services Machine Learning stack.*
- *Gain better insights in natural texts, such as customer reviews and emails.*
- *Identifies the language, key information, sentiments and topics of large number of text files for better classification and identification of trends.*

AMAZON COMPREHEND MEDICAL:

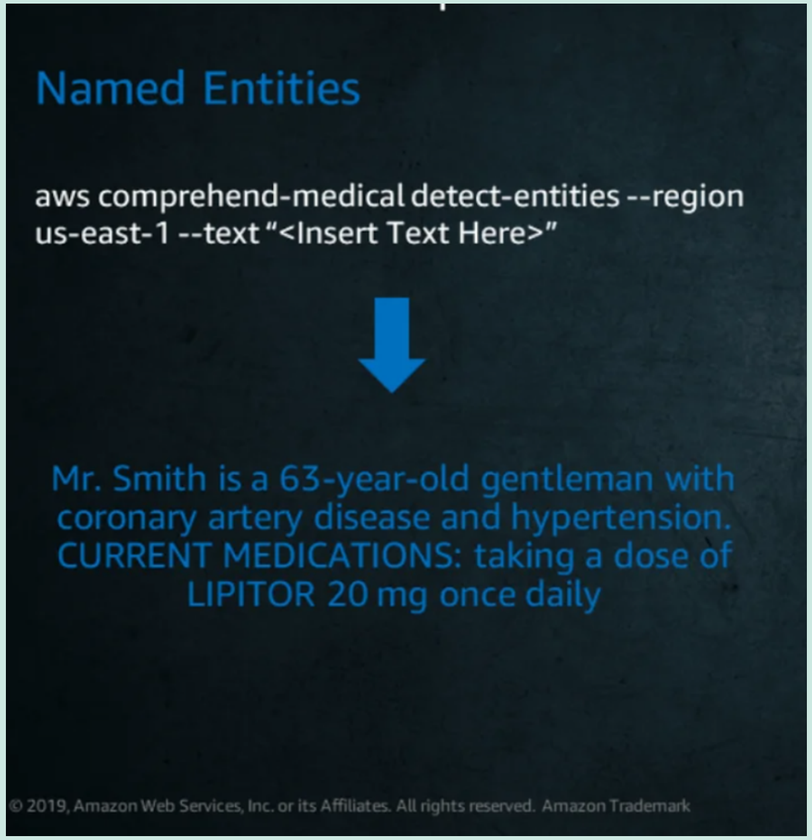
- *Feature within Amazon Comprehend that specializes in processing and extracting medical information from medical reports, logs and notes.*

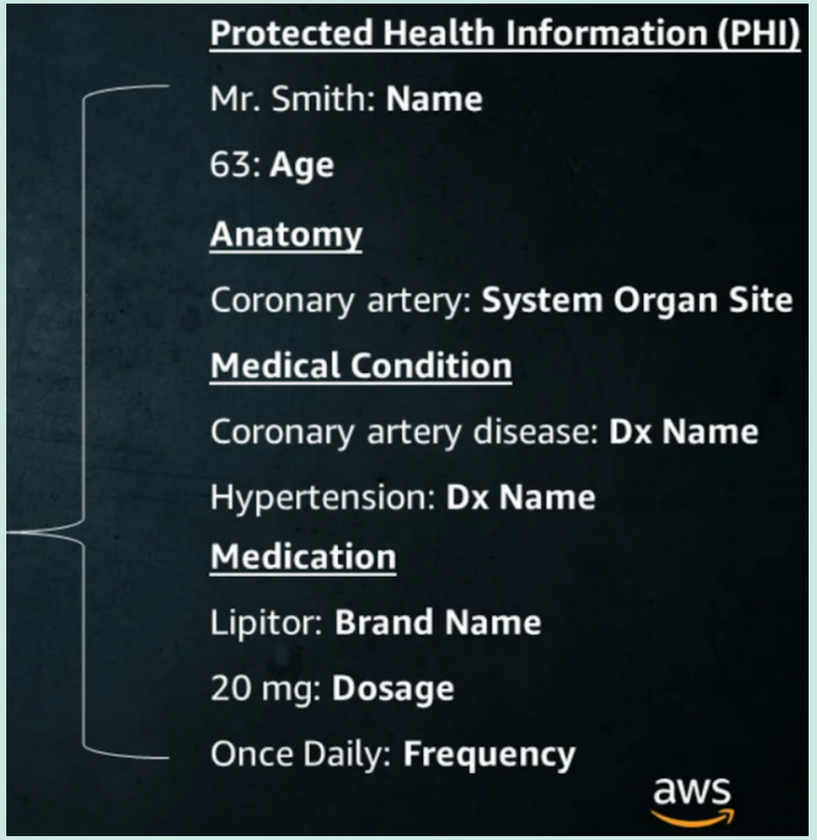


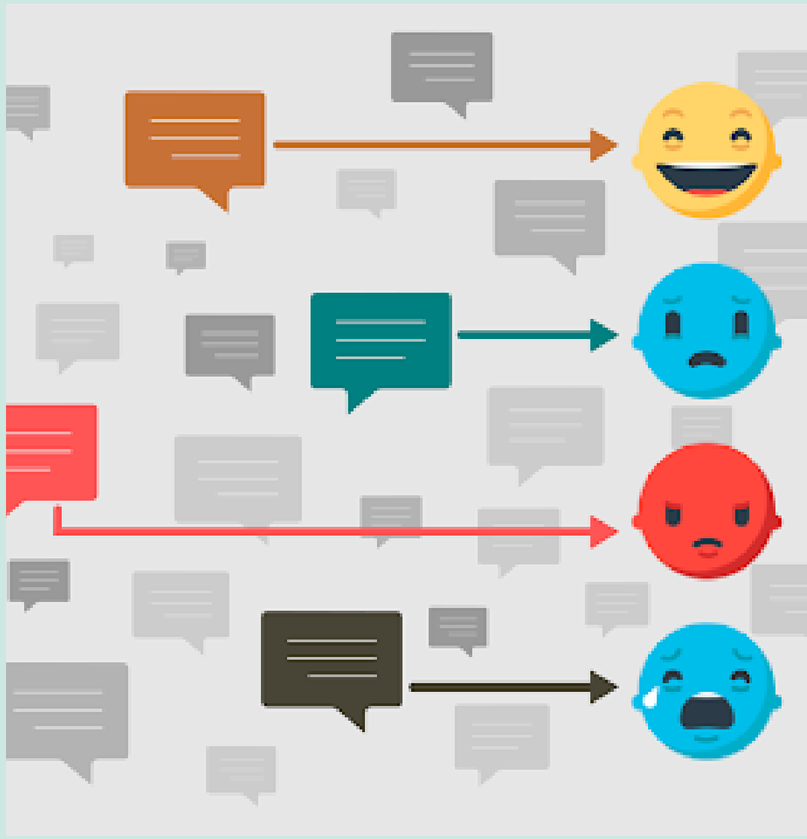


Use Cases

Medical Clinics that Provides both Online and Offline Services



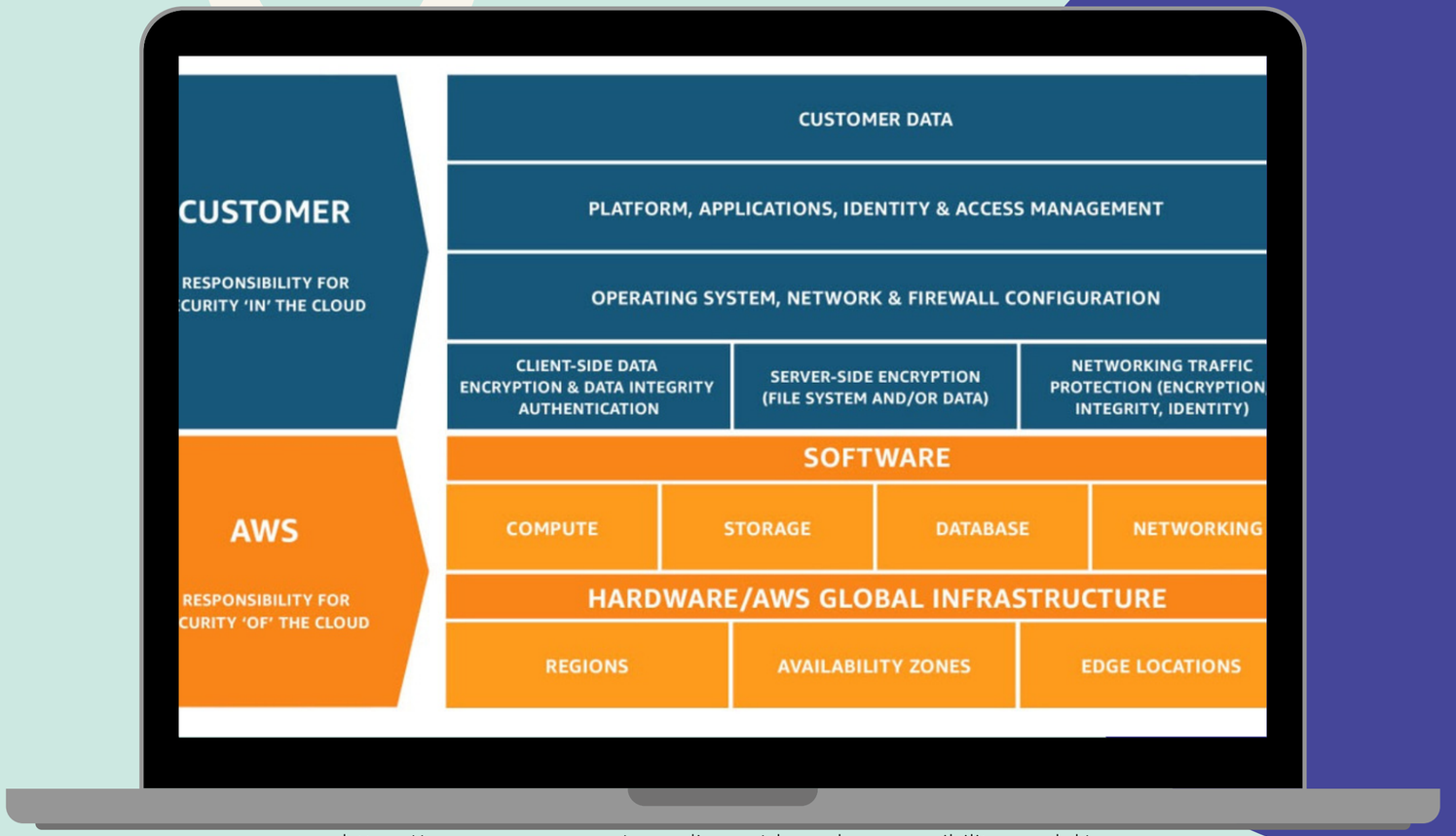




Associated Legal Notices

→

- Customer Agreement (specifically s.3 &4)
- AWS Service Terms (specifically s.50)
- AWS Acceptable Use Policy
- Amazon Machine Learning Language Service Level Agreement
- AWS GDPR Data Processing Addendum
- Shared Responsibility Model (Non-legal notice explanation)



https://aws.amazon.com/compliance/shared-responsibility-model/

Limitation of Use

01

Content must not violate any applicable law.

AWS Customer Agreement s4.2

02

Non-Medical data of EU residents requires opt-in consent to be processed on Amazon Comprehend as data may be stored outside of EU.

AWS Service Terms s50.3

03

Cannot train models with own unlabeled medical datasets using solely AWS.

AWS Service Terms s60.4

Legislation Comparison

Data Privacy Legislations	GDPR	CCPA	HIPAA	CSL
Jurisdiction	EU/UK	California (US)	USA	China
Scope	All Data	Businesses	Medical	Network Operators and "Critical Sectors"
Consent - General	Prior & Explicit	After & Implicit	N/A	Implicit, unless specified
Consent - PHI	Yes, except direct patient care	Yes, except treatment purposes	Yes, except treatment purposes	Explicit, except Public Interest Related
Right to Forgotten/Erasure	Yes	Yes	N/A	Yes, if network operator violated agreements
Penalties	~ €20 million or 4% worldwide annual revenue	~ $2,500 for unintentional, ~$7,500 for intentional violation	$100 - $50,000 per record, max $1.5 m per year	Suspension of Business &/or Max. RMB 1 m ($150k)

Data Protection Impact Assessment (DPIA)

●○○○

Need

Explain what project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA

●●○○

Process Description

- Description of the nature of the processing
- Description the scope of the processing
- Description the context of the processing
- Description of the purpose of the processing

●●●○

Consultation Process

Describe when and how you will seek individuals' views - or justify why it's not appropirate to do so

●●●●

Necessity & Proportionality

- Lawful basis for processing
- Does the processing achieve the purpose?
- How will you ensure data quality and data minimization?
- What information will you give individuals?
- How will you help to support their rights?

Identified Risks

●○○○

Profiling

Automated individual Decision-Making, including Profiling.

●●○○

Chained Consent

Patient consenting their data to the clinic, which leads to consenting processing by AWS

●●●○

Storage & Processing of Data

Time, Location, and Security of data

●●●●

Data Transfer

Different countries have a different regulations

Risk 1: Profiling

Service • Counselling sessions through text and video chats online	S	U
Potential Risk • Amazon Comprehend tagging patient transcript to involve self-harm or harm to others, which must be reported to authorities.	R	V

Use

- Process counselling session chat transcripts to obtain:
  - keywords
  - patient sentiment

Violation of Legislation

"The Data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" (GDPR 22)

Risk 1 Mitigation

- revision by human:
  - all data output, including keywords, tags and sentiments must be reviewed by a human
  - transcripts tagged with sentiments of self-harm and harm to others must be reviewed by the original therapist, or a therapist consented by the patient before performing any escalating actions
- remove unrelated information from transcripts such as:
  - residential address and/or zip code
  - race

Risk2: Chained Consent

Service • Collection and maintenance of patient data to monitor patients' physical and mental health and provide diagnoses	S	U	**Use** • Processing chat transcripts to help medical staff to monitor progress • Process medical reports to extract and auto-links to medical ontologies
Potential Risk • Chained consent leading the personal information being processed by 3rd party AWS affiliates • The more affiliates there are, the harder to trace the movement of data in order to comply with various legislations	R	V	**Violation of Legislation** • "The data subject shall have the right to obtain.... [and] the erasure of personal data concerning him or her..." (GDPR 17) • "In responding to a consumer's verified ... response to the consumer as required by the CCPA" (CCPA 999.313)

Risk2 Mitigation

- clear documentation:
  - detailed documentation of possible 3rd party affiliates of products used
  - risk analysis on 3rd parties
- identify all features that are associated with the Amazon Comprehend
  - Mechanical Turk is the 3rd party identified in the AWS ML Stack
- possible mitigations:
  - use Amazon Comprehend and Amazon Comprehend Medical as is without custom model
  - ensure staff performing the classifications are located in the same region as data collection by hiring in-house

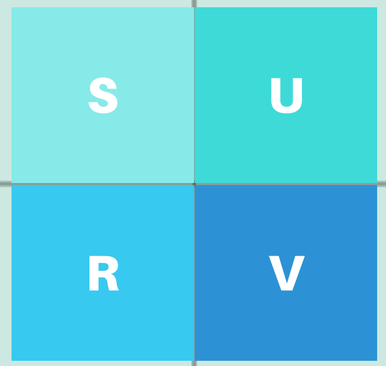
Risk3: Data Storage & Processing

Service

- Collects and stores both medical and non-medical data of patients
- Certain data are stored locally and others on cloud servers for processing

Use

- Stores and processes chat transcripts and medical reports of clinic patients for analysis



Potential Risk

- Data being deemed to be irrelevant for patient treatment purposes
- Data breach through storage
- Medical records, including personal information, may not be stored outside of regions or countries obtained

Violation of Legislation

- "... kept in a form which permits identification of data subjects for no longer than is necessary...." (GDPR 5(1)(e))
- "Critical information infrastructure.... shall store it within mainland China." (CSL 37 translated)

Risk3 Mitigation: Retention

- Different retention times for different types of data:
  - Medical Data
    - Such as: Medical reports, prescription, AWS Comprehend Medical Output, AWS Comprehend sentiment trends, etc.
    - Different jurisdictions have different requirements on how long medical records must be kept
      - California
      - China
      - Spain
    - Comply according to relevant jurisdiction regulations on medical data retention
  - Non-Medical Data
    - including:
      - Permanent address
      - AWS Comprehend output keywords, locations, etc.
    - Data retention period 12 months per CCPA 999.313

Risk3 Mitigation: Storage & Safeguard

- Data Storage Location
  - Data Localization
  - Restriction on cross-border data transfers
  - Store data obtained within the same region to mitigate risk of having different policies for each legislative jurisdictions
- Use different safeguards for different types of data prior to upload and processing with Amazon Comprehend and Amazon Comprehend Medical
  - Safe Harbor approach from HIPAA and apply I-distinct
    - removes and/or anonymize according to the 18 specific identifiers
    - case study found this method reduced individuals uniquely identifiable to be 0.072%
  - further de-identify categorical indirect identifiers
  - Blockchain

Risk4: Data Transfer

Service

- Patients can receive medical care in any of our clinics located in different parts of the world
- Send medical records to insurance companies, bank, etc

Use

- Transfer of patient related data to be processed

S U R V

Potential Risk

- In case of data breach during transfer
- Data may be obtained and subsequently stored by countries with less security legislation, diminishing the rights and control of the data subject

Violation of Legislation

"Any transfer of personal data which are undergoing processing or are intended for processing ... international organization to another third country or to another international organization." (GDPR 44)

Risk4 Mitigation

- Basis of an Adequacy Decision (GDPR 45)
  - No authorization required if transferred to a country or territory, where the European Commission have decided that they have adequate level of protection: European Economic Area
- ensure processing center is within the same region as data collection
- Transfers Subject to Appropriate Safeguards (GDPR 46)
  - Binding Corporate Rule (GDPR 47)
- Derogations for Specific Situation (GDPR 49)
  - Relevant exceptions:
    - (a) explicit consent from data subject with understanding of lack of appropriate safeguards
    - (f) transfer is necessary to protect vital interest of data subject
- explicit consent from patients prior to cross-border transferring of patient data required
  - patient must contact home clinic to verify their identity and explicitly request the transfer of data

Open Discussion Topic

●○○○

GDPR vs. HIPAA for Medical Data

How do we balance between the two?

●●○○

Harmonization of Legislations

How can our clinic maximize its efficiency under these various legislations?

●●●○

Adaptability of Changes

Is our clinic ready to adapt to any changes in legislations in the near future?

●●●●

Technology vs. Legislation

How will technology adapt to these regulations?

NEXT

Attribution of Responsibility

01

RIGHT PERSONNEL

Hire a Chief Information Security Officer (CISO) and a Data Protection Officer (DPO)

02

PROPER TRAINING

Clinic need to implement a proper training to ensure every employee knows what they are doing

03

EMPLOYEE DATA GUIDELINE AGREEMENT

To avoid any mismanagement, employees must sign clinic's data guideline agreement to strengthen their responsibilty

Allison Black

Eun Suk Hong

Deborah Cheng

Roberto Picon

Guillermo Germade

Vasilis Sagiannos

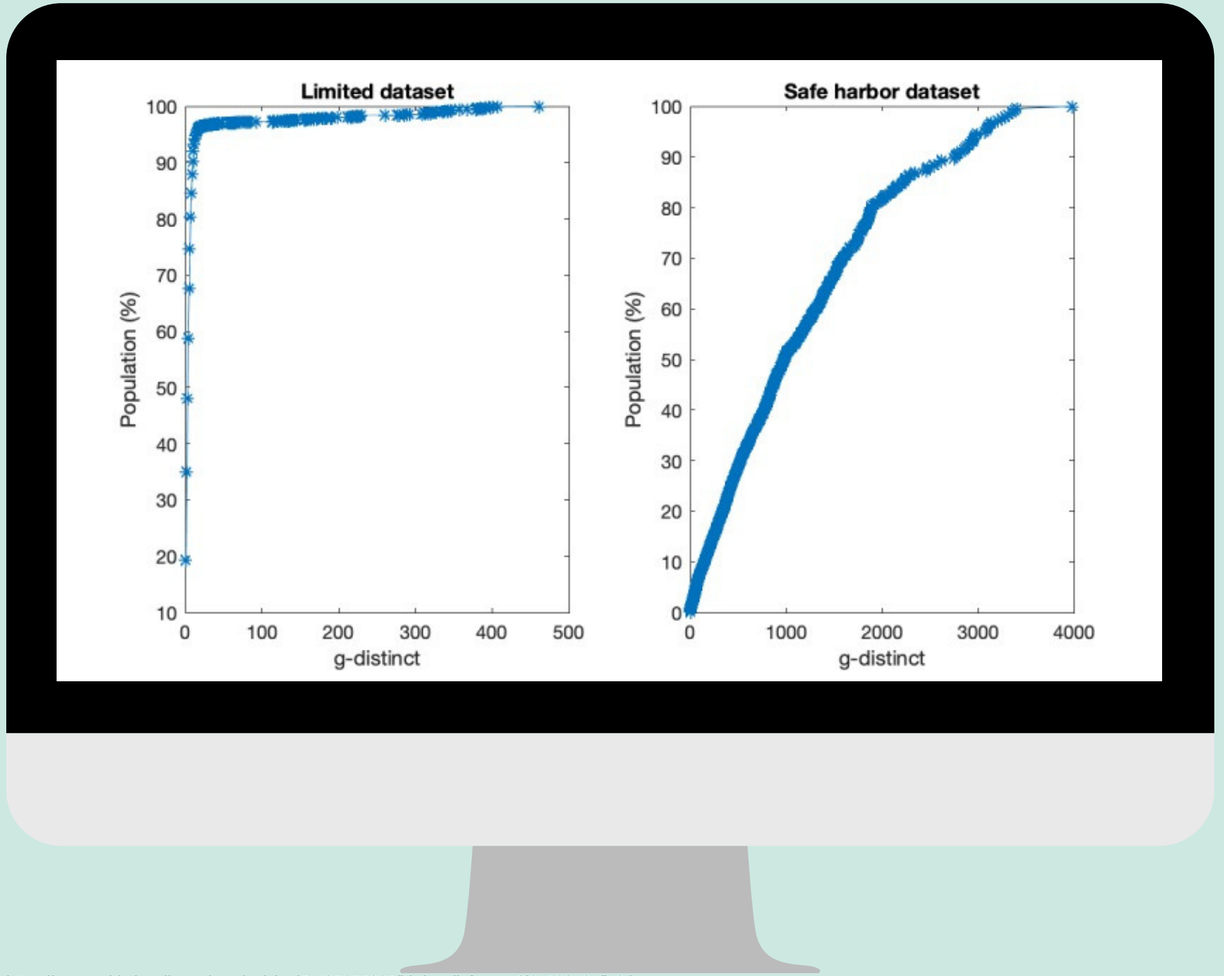
Thank You

Appendix

- Names
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health Plan
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet Protocol (IP) address number
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met.
- All geographic sub-divisons smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census
  - the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people
  - the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
- All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

https://www.hhs.gov/sites/default/files/privacysummary.pdf

Appendix



https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7055805/bin/medinform_v8i2e13046_fig2.jpg
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7055805/#:~:text=In%20China%2C%20the%20Network%20Security,personal%20information%20they%20have%20collected.

Sources

- https://aws.amazon.com/agreement/
- https://aws.amazon.com/service-terms/
- https://aws.amazon.com/aup/
- https://aws.amazon.com/machine-learning/language/sla/
- https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
- https://aws.amazon.com/compliance/shared-responsibility-model/
- https://aws.amazon.com/comprehend/?nc2=h_ql_prod_ml_comp
- https://gdpr-info.eu/art-45-gdpr/
- https://gdpr-info.eu/art-46-gdpr/
- https://gdpr-info.eu/art-49-gdpr/
- https://gdpr-info.eu/art-44-gdpr/
- https://gdpr-info.eu/art-17-gdpr/
- https://gdpr-info.eu/art-5-gdpr/
- https://gdpr-info.eu/art-30-gdpr/
- https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf
- https://www.privacy-regulation.eu/en/article-47-binding-corporate-rules-GDPR.htm
- https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/#:~:text=Article%2037%3A%20Critical%20information%20infrastructure,store%20it%20within%20mainland%20China.
- https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7055805/#:~:text=In%20China%2C%20the%20Network%20Security,personal%20information%20they%20have%20collected.
- https://www.activemind.legal/legislation/gdpr/article-22/
- https://www.hhs.gov/sites/default/files/privacysummary.pdf
- https://www.youtube.com/watch?v=T63LDIRbwxw&t=983s&ab_channel=AWSOnlineTechTalks

Sources

- https://pernot-leplay.com/data-privacy-law-china-comparison-europe-usa/#:~:text=While%20China's%20Cybersecurity%20Law%20and,where%20just%20consent%20is%20used.
- https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act#:~:text=Personal%20data%20in%20Singapore%20is,and%20care%20of%20personal%20data.&text=The%20PDPA%20provides%20for%20the,Not%20Call%20(DNC)%20Registry.
- https://www.compliancejunction.com/gdpr-for-us-companies/#:~:text=US%20companies%20within%20the%20scope,with%20all%20the%20Regulation's%20requirements.&text=Compliance%20will%20be%20mandatory%20for,take%20place%20outside%20the%20Union.
- https://www.cookiebot.com/en/ccpa-vs-gdpr/
- https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf
- https://www.dlapiperdataprotection.com/index.html?c2=CN&c=SG&t=law
- https://ico.org.uk/for-organisations/in-your-sector/health/health-gdpr-faqs/
- https://www.fairwarning.com/insights/blog/gdpr-and-hipaa-compliance-what-are-the-differences-and-how-can-i-work-towards-compliance#:~:text=The%20key%20difference%20between%20GDPR,on%20protecting%20EU%20citizens%27%20PII.&text=In%20contrast%2C%20HIPAA%20is%20focused,PHI)%20within%20the%20United%20States.
- https://securityboulevard.com/2019/08/what-is-the-ccpa-and-who-must-comply-the-california-consumer-privacy-act-explained/#:~:text=As%20for%20fines%20and%20enforcement,the%20preset%20%242%2C500%20maximum%20fine.