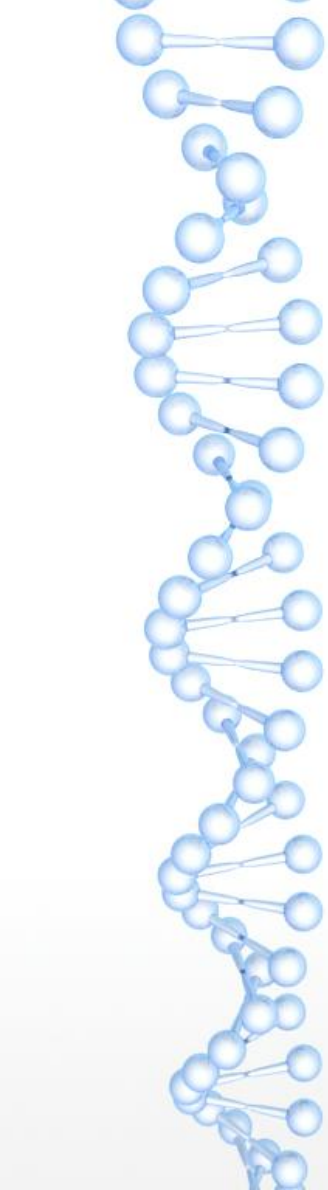
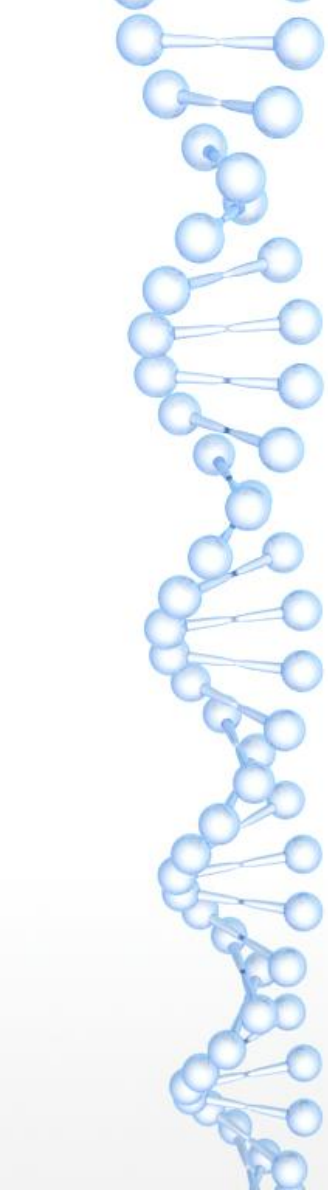


ISSA Raleigh, NC Chapter
December 5, 2018

Mauricio

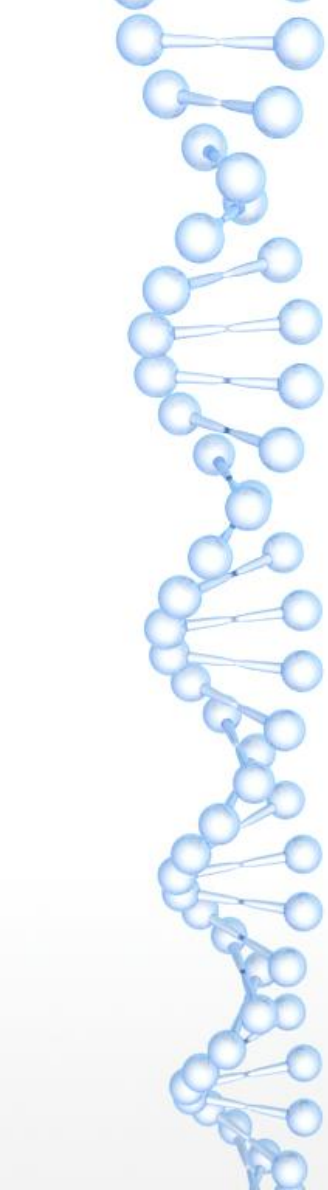
XXXXXXXXXX

Valdez Ladd
MBA-ISM, CISSP, CISA, CIW-SP



Goal:

Add Data Privacy Impact testing to your cybersecurity management for audit and compliance

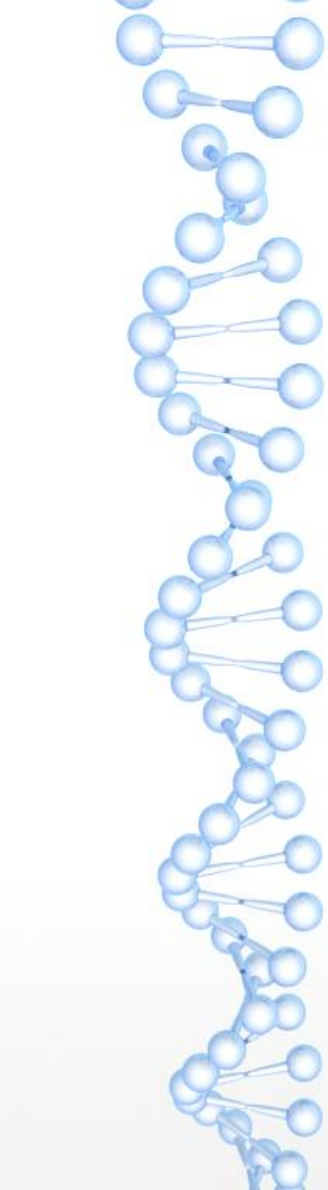


Number of Data Privacy laws are increasing

- USA by state, All 50 now

- industry PCI, HIPAA

- internationally EU GDPR, PIPEDA



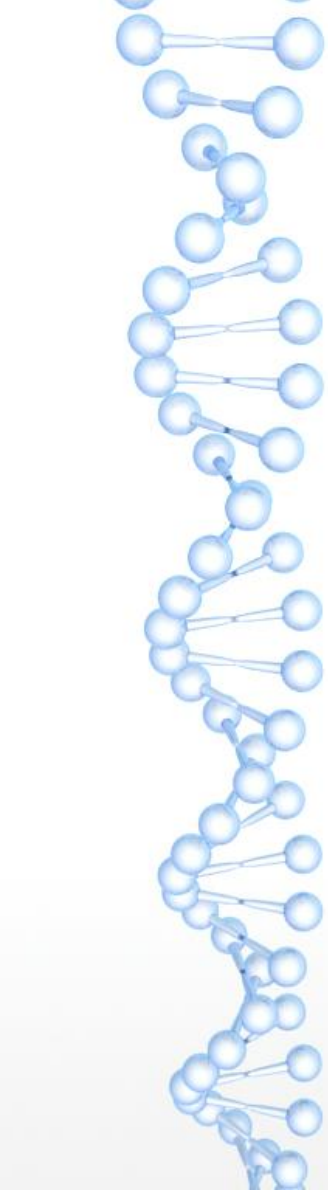
Annually cybersecurity breaches: millions $$ & millions of records

New executive: Chief privacy officers (CPO)

Corporate executives fired - Equifax, Yahoo,

Business partners, customers & 3rd party companies

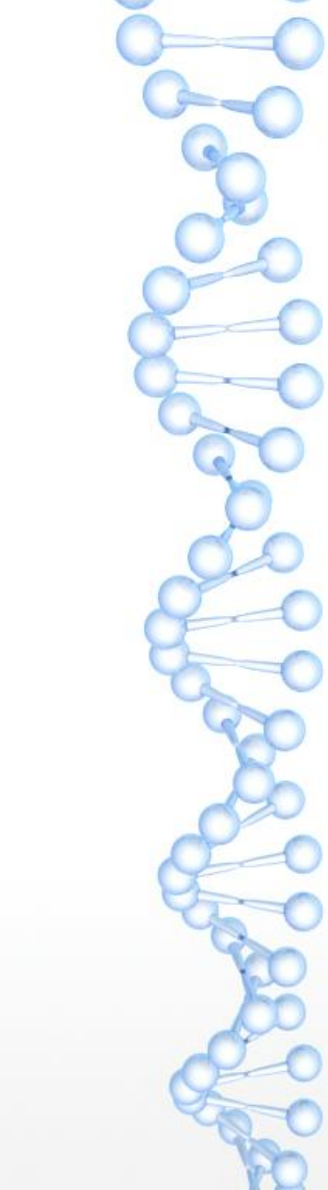
Cloud Services - Amazon AWS, Microsoft Azure, Google



CIA triad [Confidentiality, Integrity, & Availabilty]

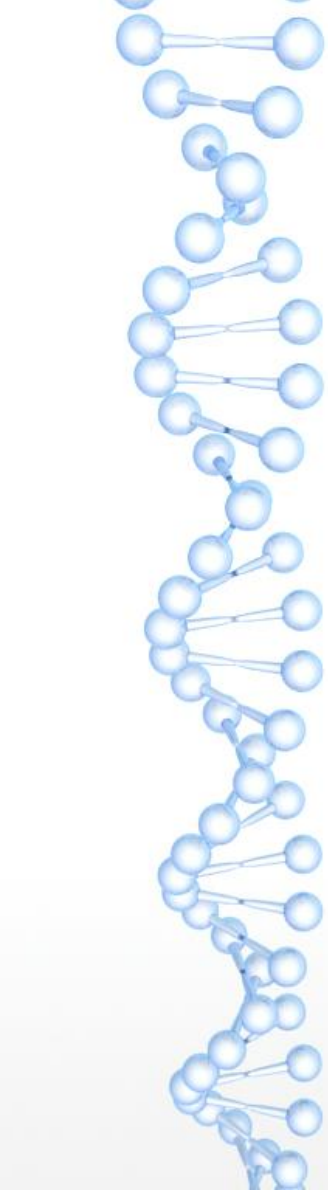
- protects data & information systems

Data privacy - person's ability to control personally identifiable information (PII)



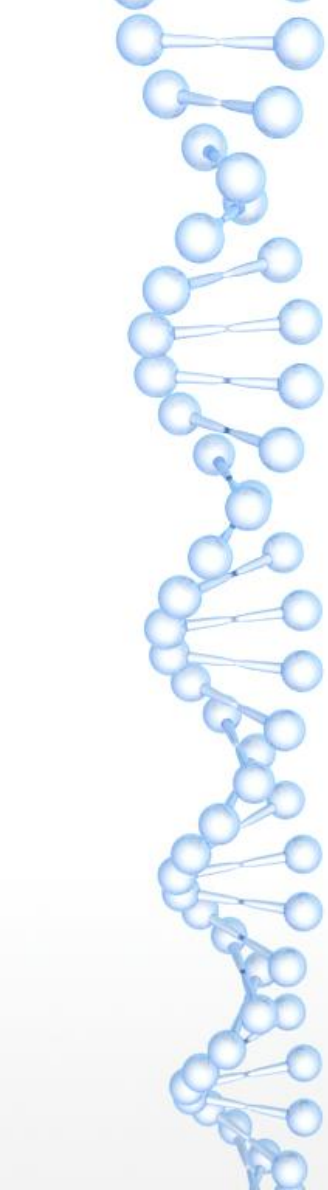
Mitre Corp. data privacy:

- Accountability
- Integrity
- Aggregation
- Confidentiality
- Destruction / Retention



Data Privacy Laws & Standards

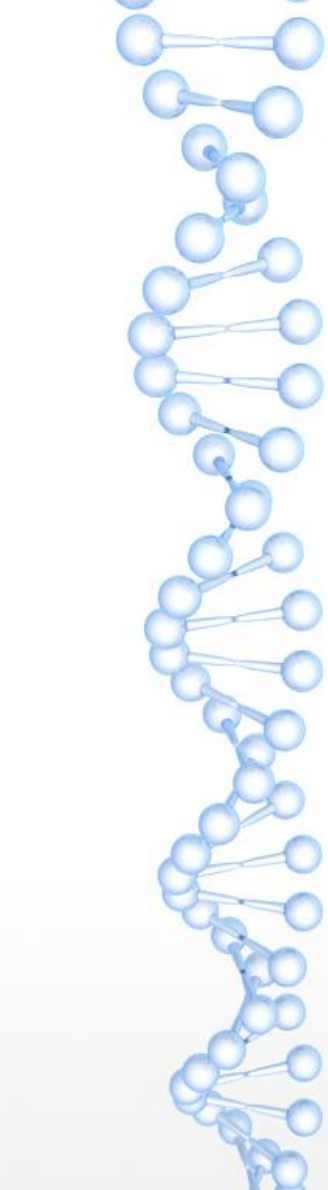
HIPAA, PCI DSS, & EU GDPR (May 2018)



HIPAA - Health Insurance Portability Accountability Act

- Privacy Rule (data privacy)
- Security Rule (data security)

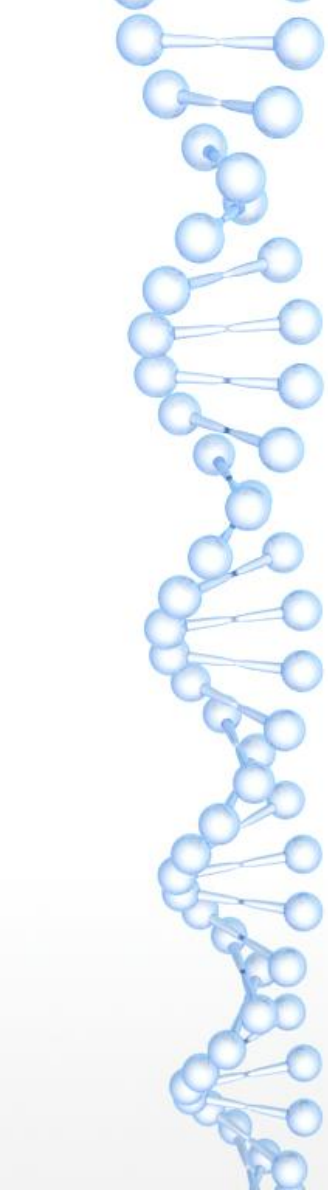
Covered entities & business associates:
OCR audits



PCI DSS
(Payment Card Industry Data Security Standard)

- All entities that store, processes, and /or transmit cardholder data

- both technical & operations systems components in/ or connected to cardholder data.



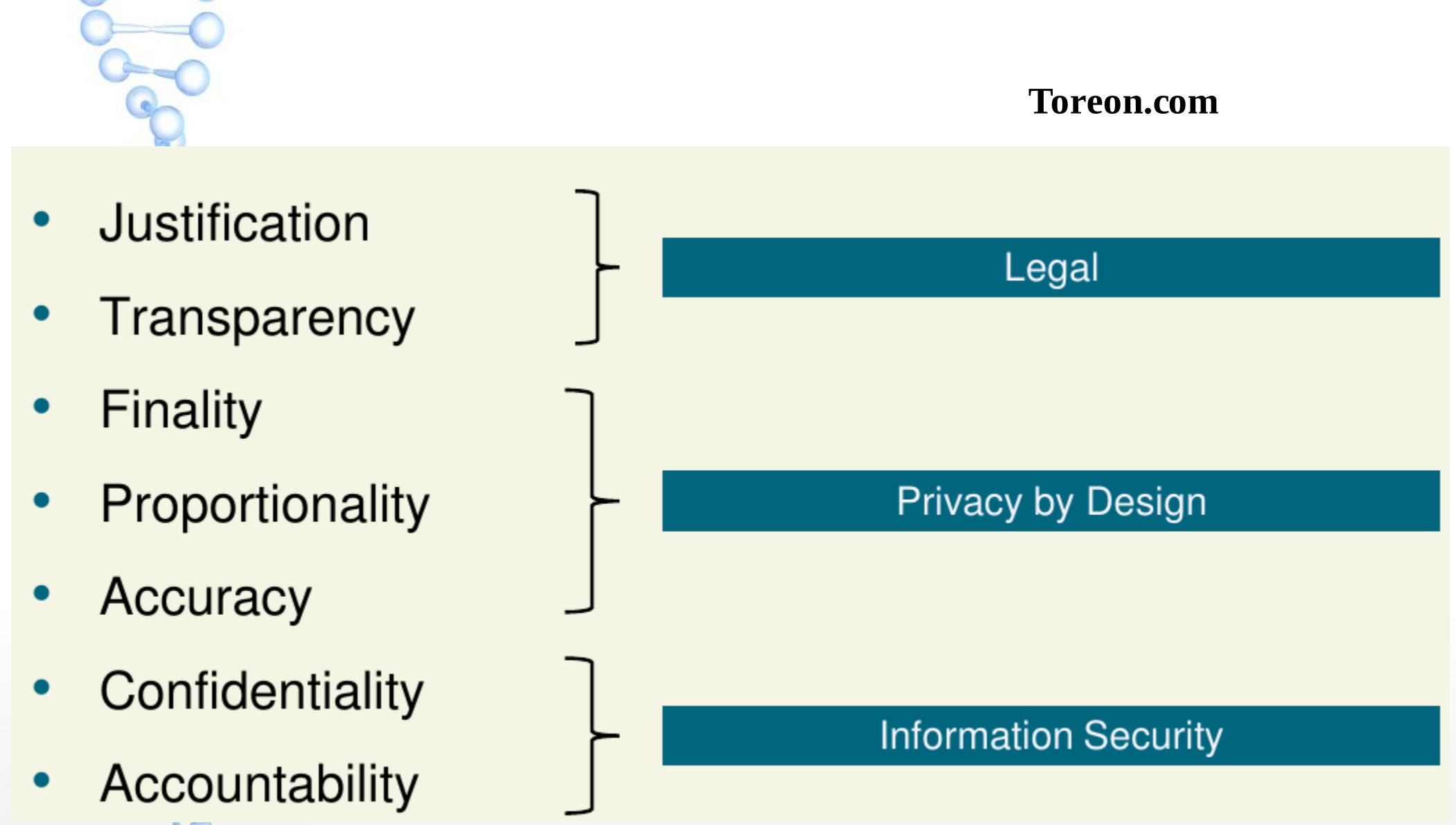
EU GPDR

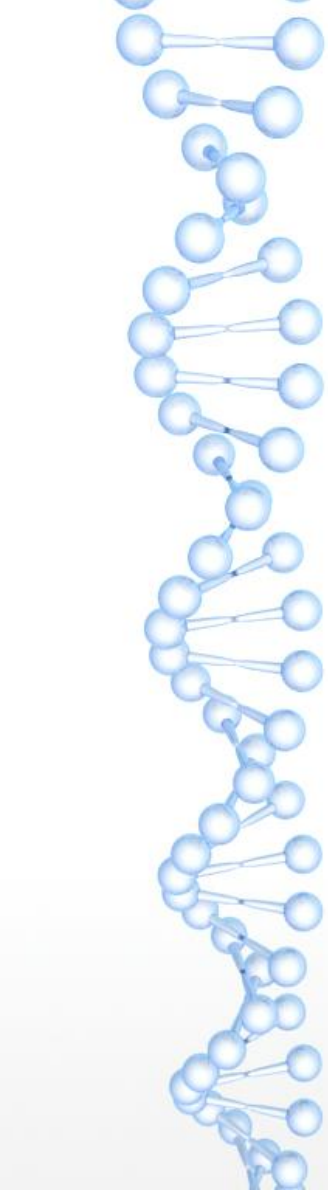
(European Union General Data Protection Regulations)

7 Principles

(3 – CIA triad)

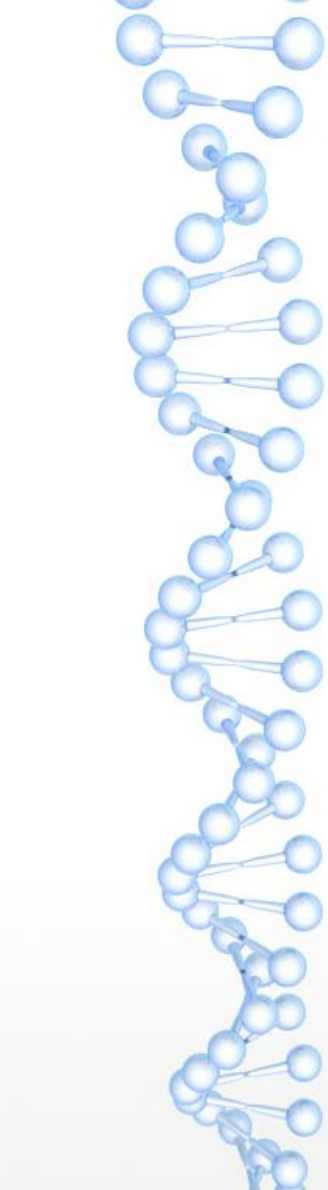
- Accuracy
- Confidentiality
- Accountability


Justification
Transparency
Finality
Proportionality
Accuracy
Confidentiality
Accountability
Legal
Privacy by Design
Information Security



EU GDPR: Article 35

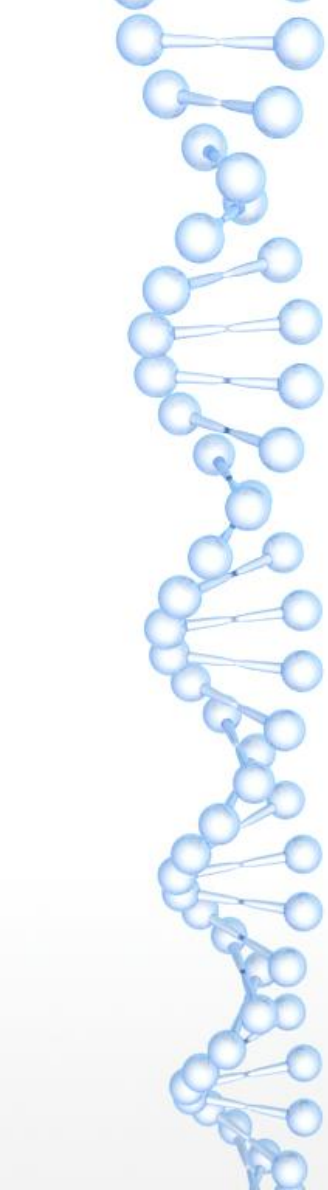
Data Privacy Impact Assessment (PIA) and Risk Assessment



Dept. Health & Human Services Office of Civil Rights (OCR) Audit

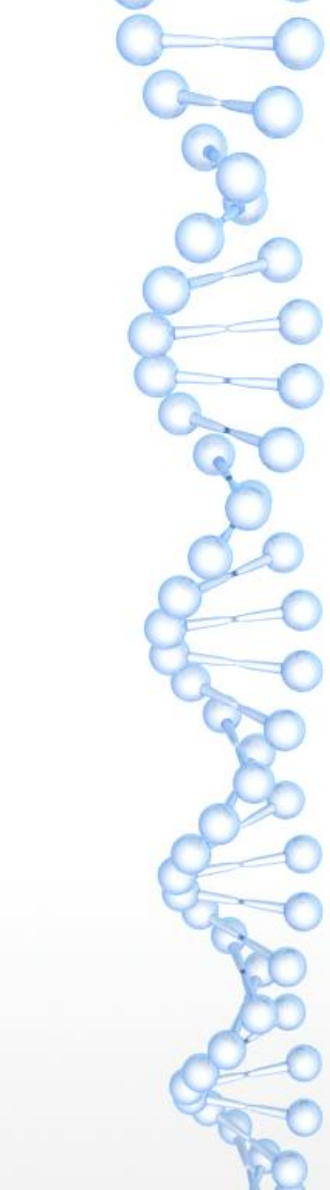
- HIPAA: Title II & III of E-Government of 2002 required of US government agencies

- HIPAA: Covered Entities (healthcare businesses, suppliers)



OWASP - Top 10 Privacy Risks

P1 Web Application Vulnerabilities
P2 Operator-sided Data Leakage
P3 Insufficient Data Breach Response
P4 Insufficient Deletion of personal data
P5 Non-transparency Policies, Terms, and Conditions



OWASP Top 10

P6 Collection of data not required for the primary purpose

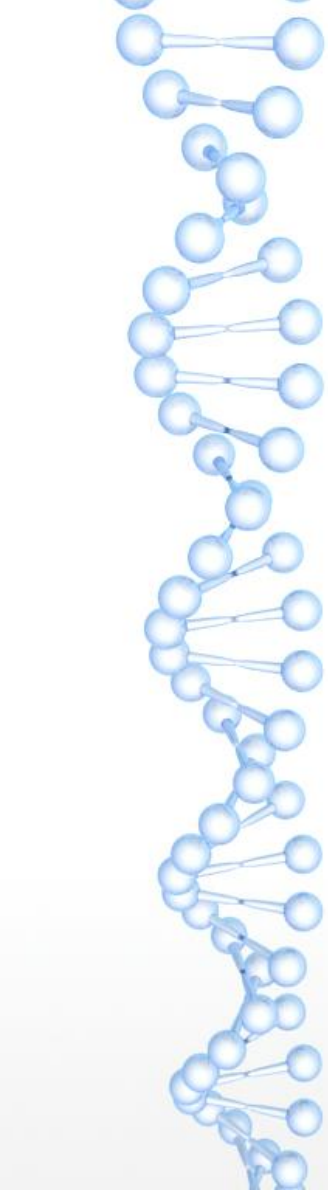
P7 Sharing of data not requried for the primary purpose

P8 Sharing of data with third party

P9 Outdated personal data

P10 Insecure Data transfer

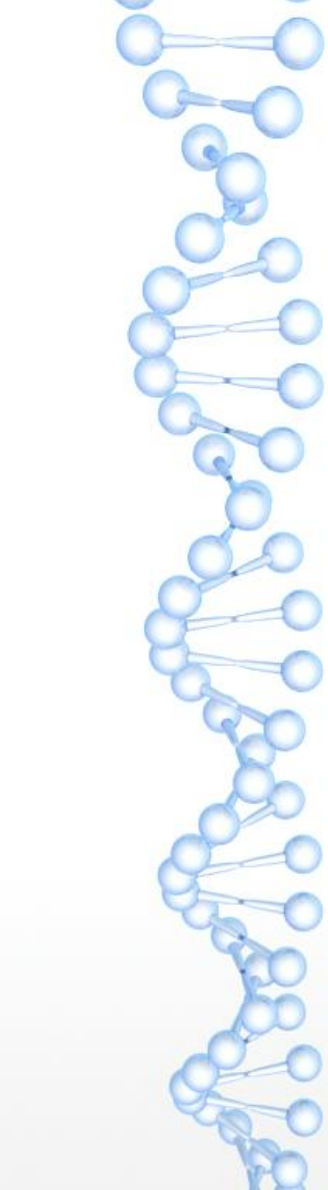
* EU Privacy Shield 2019, EU GDPR



OWASP Top 10 – Privacy Test Demo

Mauricio

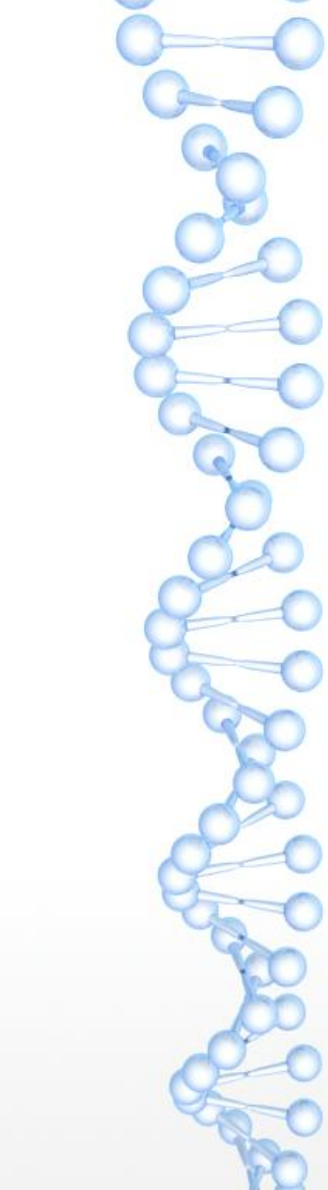
1.
2.
3.



OWASP Top 10 – Privacy Test Demo

Mauricio

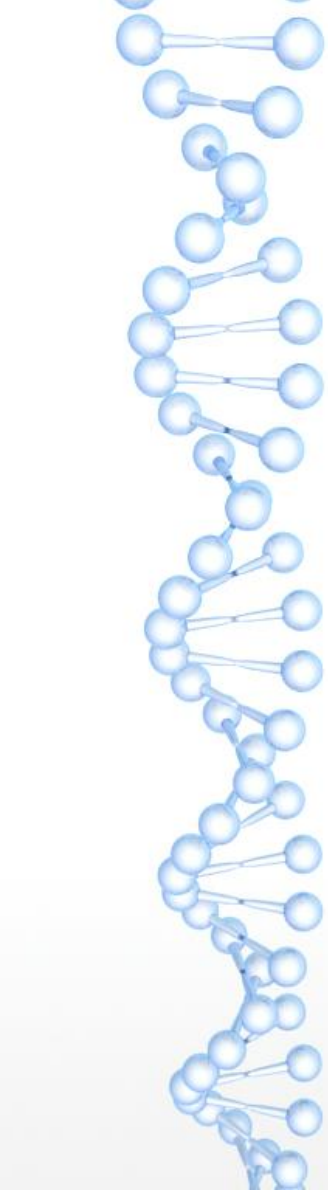
1.
2.
3.



OWASP Top 10 – Privacy Test Demo

Mauricio

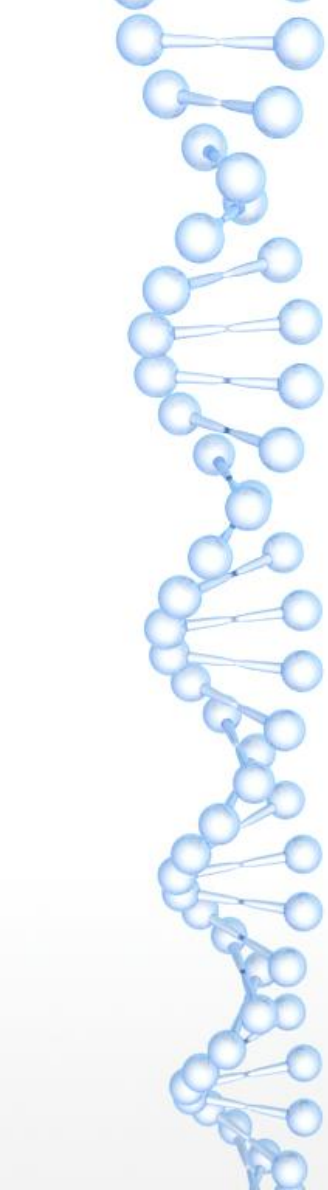
1.
2.
3.



OWASP Top 10 – Privacy Test Demo

Mauricio

1.
2.
3.



Questions?

Thank you.