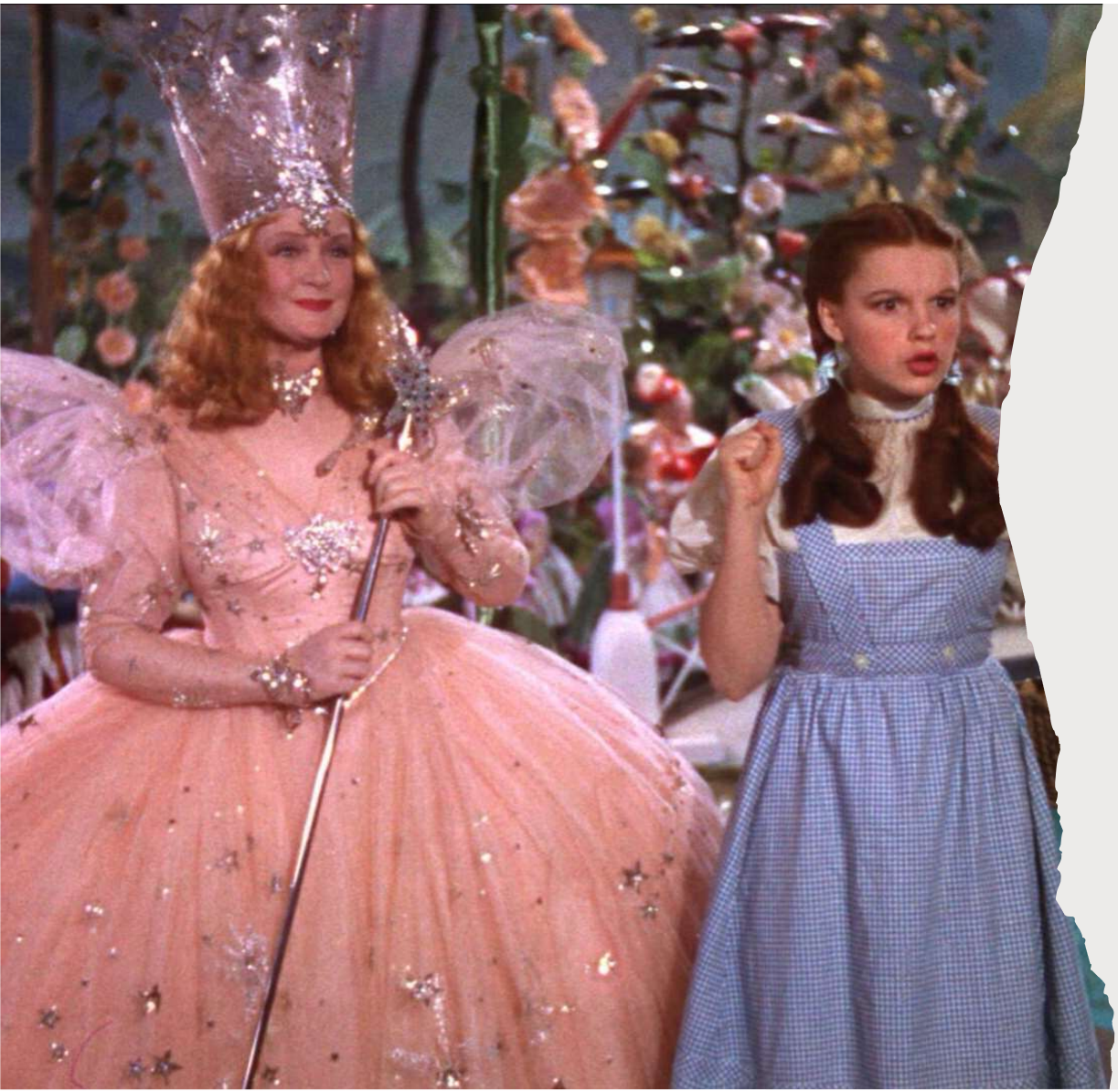
GDPRs, & PCI-DSSs, & HIPAAs, OH MY:

UNTANGLING COMPLIANCE SO YOU DON'T GET SCARED

Jennie.ocken.org



CONSULT YOUR OWN ADVISOR

- I am not a lawyer
- I am not a compliance officer
- I am not a security officer
- I am not a privacy officer
- More importantly, I am not ***your*** lawyer, compliance officer, security officer, or privacy officer

- YMMV

THIS IS PART OF YOUR JOB

WHY WORK IN A REGULATED SPACE

- Moat
- Disruption
- Differentiation
- Imposed
- No Choice

WHEN TO RAISE A FLAG

- Lack of basic internet security
- Data not encrypted, de-identified, clearly protected
- Lack of policies
- Lack of training
- No process to notify users in case of a breach
- "We don't need to worry about that, we are _____."
  - Too small
  - A startup
  - Not in a particular location
  - Not in a particular vertical
  - Working in crypto
  - A disruptor
  - Moving fast and breaking things

GDPR

+ CALIFORNIA, VIRGINIA, CANADA, SINGAPORE, NEW ZEALAND, CHINA, BRAZIL, THAILAND...

TL;DR THAT TLA

- General Data Protection Regulation (GDPR) approved by the European Parliament on April 14, 2016; went into effect on May 25, 2018
- Gold standard for data privacy laws
- Written with an actual understanding of technology and the internet
- Extremely expansive
- "GDPR" has become the shorthand for most data privacy laws across the world

GDPR OBJECTIVES

Lawfulness, fairness and transparency

Purpose limitation / Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality (security)

Accountability

WHO IS IMPACTED?

a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed;

or

a company established outside the EU and is offering goods/services (paid or for free) or is monitoring the behaviour of individuals in the EU.

ROLES

Controller

- Determines the purposes and means of the processing of personal data
- Could be multiple entities working together to make decisions as joint controllers
- Does not necessarily have to be in possession of the data to still have requirements under GDPR

Processor

- Processes personal data on behalf of the controller including subcontractors of a processor
- Serves the controller's interests rather than their own
- May make its own day-to-day operational decisions but should only process personal data in line with a controller's instructions
- If a processor acts without the controller's instructions in such a way that it determines the purpose and means of processing, including to comply with a statutory obligation, it will be a controller in respect of that processing and will have the same liability as a controller.

WHAT TYPES OF DATA

- Basic identity information
  - User-generated data like social media posts
  - Personal images uploaded to websites
  - Medical records
  - Other uniquely personal information commonly transmitted online
- Web data
  - Location
  - IP address
  - Cookie data
  - RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation
- Any information that relates to an identified or identifiable living individual

USERS HAVE THE RIGHT TO...

Access	Be Informed	Data Portability	Be Forgotten
Object	Restrict Processing	Be Notified	Rectification

WHAT DO I NEED TO DO?

- Appoint a Data Protection Officer (if you need one)
- Review GDPR
- Complete an information audit
- Determine your lawful basis for processing data
- Implement processes
- Establish documentation
- Implement training and policies

IMPLEMENT PROCESSES

- Opt-ins and privacy policy availability
- Export my data option
- Delete my data option
- Correct my data option
- Basic internet security
  - De-identify data
  - Encrypt in transit and at rest
  - Only keep data necessary to the operations of the software
  - Limit access to protected data
  - Notify if a breach happens

ESTABLISH DOCUMENTATION

- Data protection policy
- Training policy
- Information security policy
- DPIA (data protection impact assessment) procedure
- Retention of records procedure
- Subject access request form and procedure
- Privacy procedure
- International data transfer procedure (where relevant)
- Data portability procedure (where relevant)
- Complaints procedure
- Privacy notice

RESOURCES

- The EU's GDPR site: https://gdpr.eu/
- The Legal Text: https://gdpr-info.eu/
- European Commission's break down of the rules: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en
- California's CCPA site: https://oag.ca.gov/privacy/
- Helpful blog post:
  - https://cloudian.com/guides/data-protection/gdpr-data-protection/
  - https://www.osano.com/articles/gdpr-compliance-regulations
  - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
  - https://www.itgovernance.co.uk/blog/how-you-can-demonstrate-gdpr-compliance
  - https://www.british-assessment.co.uk/insights/how-to-comply-with-gdpr/

PCI-DSS

TL;DR THAT TLA

- Payment Card Industry Data Security Standard, version 1.0 rolled out December 15, 2004
- Not a law. A standard that is enforced by fines and loss of access to credit card processing
- PCI SSC –The PCI Security Standards Council
- Applies to any organization, regardless of size or number of transactions, that accepts, transmits, or stores cardholder data
- Different levels of requirements based on size and kinds of data interactions

PCI-DSS OBJECTIVES

Secure Network and Systems

Protect Cardholder Data

Vulnerability Management Program

Strong Access Control Measures

Monitor and Test Networks

Information Security Policy

WHO IS IMPACTED?

- Anyone who takes payments from one of the following credit card issuers who make up the PCI-SSC:

American Express

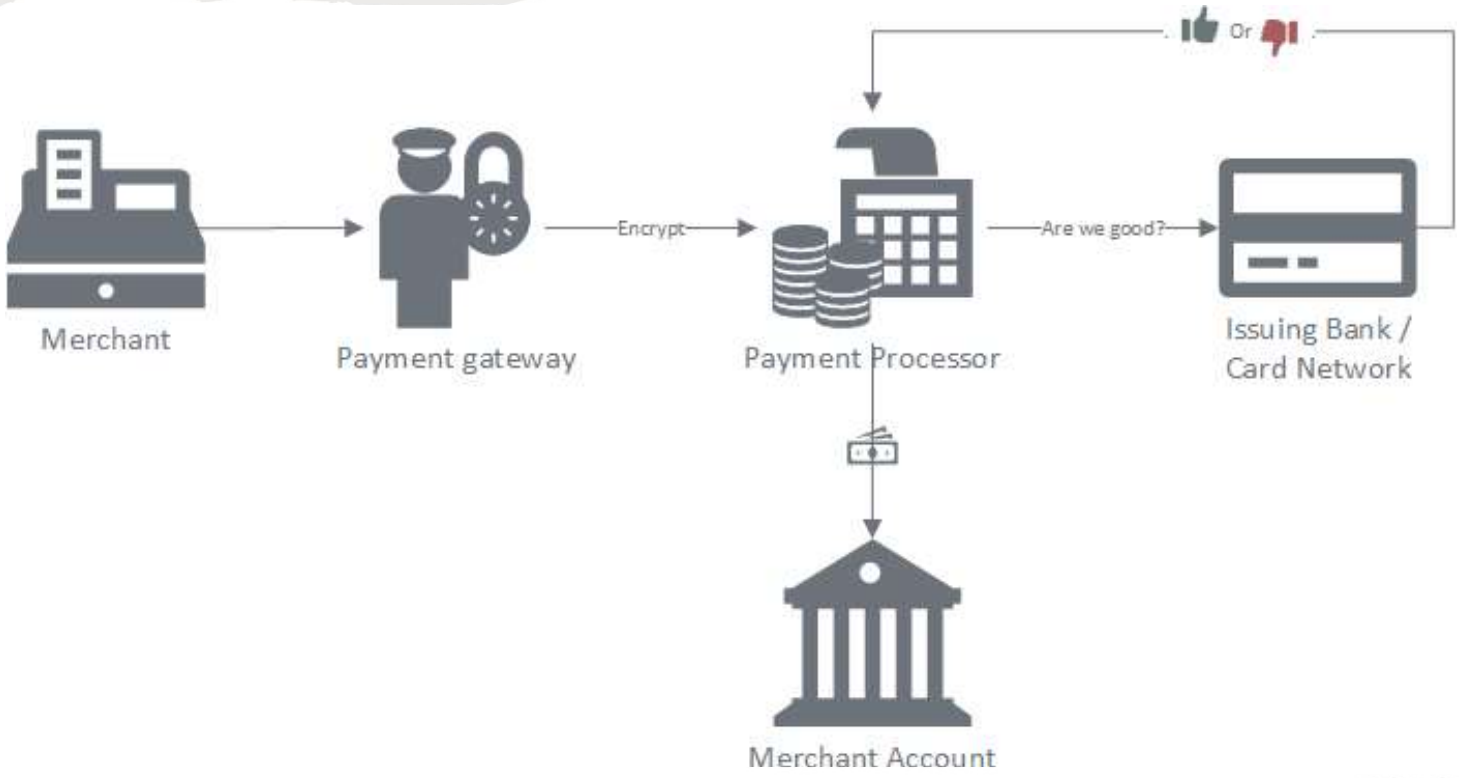
Discover

JCB

MasterCard

Visa International

1-MINUTE ON CREDIT CARD STRUCTURE AND ROLES



ROLES

Standalone Device

- Standalone, dial-up payment terminal (1,2)
- Payment device connected only to a processor (3,4)
- Payment terminal connected to an electronic cash register or till and the electronic cash register or till is connected only to a processor (5)
- PCI listed SCR (secure card reader) attached to a mobile device (12,13)
- PCI-listed P2PE Solution (15)

Interconnected System

- Payment terminal that is connected to other systems in your network (6,7,8)
- Via e-commerce (9,10,11)
- Virtual terminal (14)

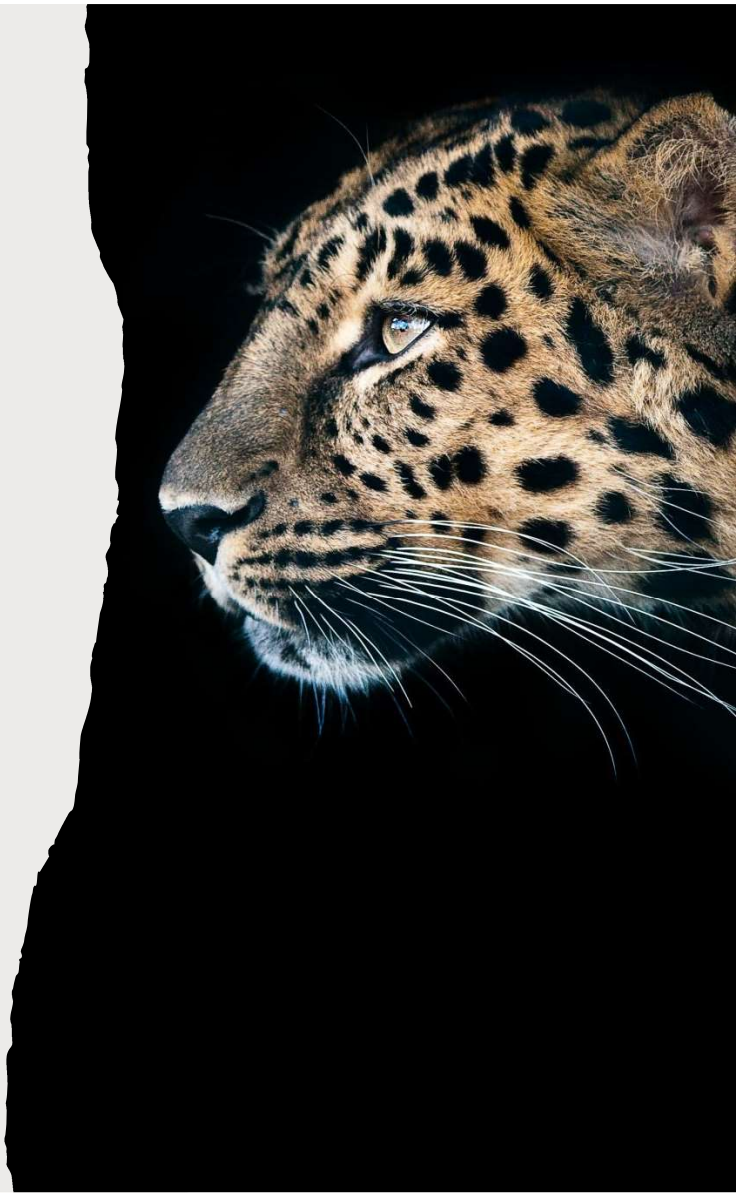
WHAT TYPES OF DATA

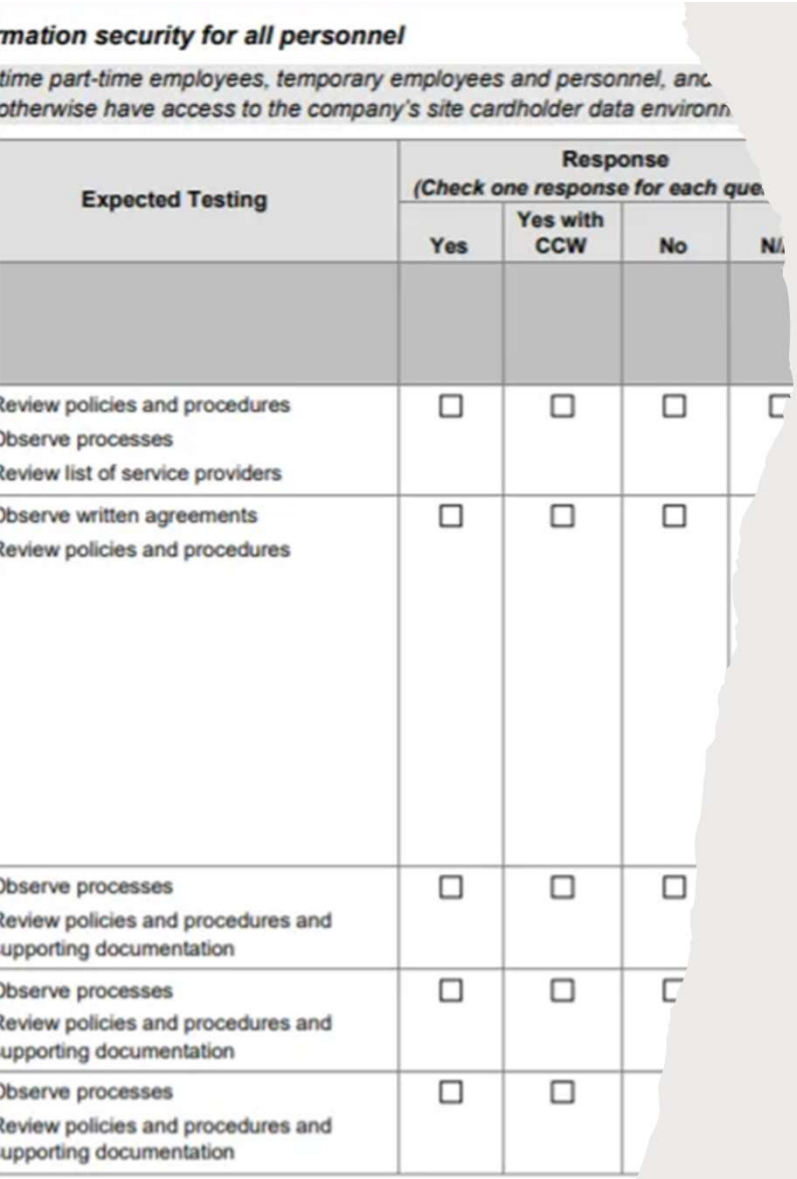
- Primary Account Number (PAN)
- Cardholder name
- Expiration date
- Service code

- Sensitive Authentication Data:
  - Magnetic stripe data
  - CAV2 / CVC2 / CVV2 / CID
  - PINs or PIN blocks

HOW TO COMPLY

- Basic Internet Security
  - Use strong passwords and change default ones
  - Install patches from your vendors
  - Don’t give hackers easy access to your systems
  - User ant-virus software
  - Scan for vulnerabilities and fix issues
  - Protect your business from the internet
- Manage and Protect Data
  - Isolate cardholder data from other systems
  - Protect your card data and only store what you need
  - Restrict access to cardholder data based on business need to know
  - Make sure your data is useless to criminals (e.g. encrypt)





rmation security for all personnel

time part-time employees, temporary employees and personnel, and
otherwise have access to the company's site cardholder data environ

Expected Testing	Response (Check one response for each que			
	Yes	Yes with CCW	No	N/
Review policies and procedures Observe processes Review list of service providers	☐	☐	☐	☐
Observe written agreements Review policies and procedures	☐	☐	☐	
Observe processes Review policies and procedures and supporting documentation	☐	☐	☐	
Observe processes Review policies and procedures and supporting documentation	☐	☐	☐	
Observe processes Review policies and procedures and supporting documentation	☐	☐		

HOW TO COMPLY

- Use a secure system or a vendor who specializes in PCI
  - Inspect payment terminals for tampering
  - Protect in-house access to your card data
  - Use secure payment terminals and solutions
  - Use trusted business partners and know how to contact them
- Employee policies and procedures
  - Maintain a policy that addresses information security for all personnel
  - Notify if a breach happens
  - Regular training
- Annual attestation report and scan (if required)
- Compliance officer… maybe

RESOURCES

- Full text of the standard: https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf
- PCI-SSC Official Site
  - Safe payments Guide: https://listings.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
  - Self Assessment Tool: https://listings.pcisecuritystandards.org/pci_security/small_merchant_tool/
- PCI-SCC Merchant's site: https://www.pcisecuritystandards.org/merchants/
- Helpful Blog sites
  - https://pcijourney.com/
  - https://www.pcicomplianceguide.org/

HIPAA

TL;DR THAT TLA

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-19
- Privacy Rule added in December 2000, Security Rule added in February 2003
- National standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge
- Attempting to improve efficiency in the healthcare industry and portability of health insurance
- Only applies to covered entities and business associates

HIPAA OBJECTIVES

Health insurance portability

Reduce healthcare fraud and abuse

Standards for health information

Security and privacy of health information

Administrative simplification

Patient access to medical records

WHO IS IMPACTED

- Individuals or entities that transmit protected health information for transactions for which the Department of Health and Human Services has adopted standards.
  - Healthcare claims
  - Payment and remittance advice
  - Healthcare status
  - Coordination of benefits
  - Enrollment and disenrollment
  - Eligibility checks
  - Healthcare electronic fund transfers
  - Referral certification and authorization

ROLES

Covered Entities

- Healthcare Providers or Pharmacists
- Service that handles health information (clearinghouse)
- Health plan or health insurance

Business Associate

- Business working with a Covered Entity that creates, receives, maintains, or transmits Protected Health Information (PHI)
- Subcontractor for another business associate if they interact with PHI
- Health information organization
- E-prescribing gateway

TYPES OF DATA

- Name
- Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Finger or voice print
- Photographic image - Photographic images are not limited to images of the face.
- Any other characteristic that could uniquely identify the individual

HOW TO COMPLY

- Designate HIPAA Privacy and Security Officer(s)
- Identify PHI in your systems and map data flows
- Protect PHI to minimize risks to "reasonable and appropriate" levels and prevent any "reasonably anticipated" breach
  - Isolate, de-identify, and encrypt data
  - Reduce access to only data required to do their job (role based access controls) and log access
  - Basic internet security (Malware and ransomware protections, Password policy, shut down accounts)
- Retain PHI and automate monitoring and reporting
- Document policies and procedures and "regularly" train workforce
- Business associate agreement with any contractors who interact with PHI

PRIVACY POLICIES

- Patient Rights
  - Accounting of Disclosures of Protected Health Information
  - Amendment of Protected Health Information
  - Complaints
  - Notice of Privacy Practices
  - Patient Access to Protected Health Information
  - Request for Alternative Communication
  - Restrictions to Permitted Uses and Disclosures of Protected Health Information
- Uses and Disclosures of Protected Health Information
  - Authorization for Release of Protected Health Information
  - Disclosure of Alcohol and Substance/Drug Abuse Records
  - Marketing and Fundraising
  - Minimum Necessary for Uses and Disclosures of Protected Health Information
  - Responding to Subpoena and Court Order
  - Use and Disclosure of Limited Data Sets
  - Uses and Disclosures of Protected Health Information for Research
  - Uses and Disclosures of Protected Health Information for the Directory
  - Uses and Disclosures of Protected Health Information Permitted and Required by Law without Authorization
- General Rules
  - Business Associate and Business Associate Agreement
  - Emailing Protected Health Information
  - Faxing Protected Health Information
  - Personal Representatives
  - Safeguarding and Storing Protected Health Information
  - Verification of Identity and Authority of Persons Requesting Protected
- Health Information
  - Administrative
  - Breach of Protected Health Information and Breach Notification
  - De-Identification of Protected Health Information
  - Designed Record Set
  - Privacy Official Designation
  - Sanctions
- Documentation
  - Destruction of Protected Health Information
  - Retention of Protected Health Information

SECURITY POLICIES

- HIPAA Information Security Policy
- Business Associate Compliance Monitoring
- Business Continuity Plan
- Business Impact Analysis
- Data Integrity Procedures
- Employee Handbook
- Firewall Configuration Standards
- Incident Response
- Job Descriptions
- Network Time Protocol (NTP) Configuration Procedures
- Operating Procedures
- Physical Security Procedures
- Risk Treatment Proposal
- Security Awareness Training Procedure
- Vulnerability Discovery and Risk Ranking
- Workstation Functions

RESOURCES

- Full Text of Law: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html
- Useful Government Sites:
  - Department of Health and Human Services: https://www.hhs.gov/hipaa/for-professionals/index.html
  - Center for Medicare and Medicaid Guide: https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA
  - Security Risk Assessment Tool: https://www.healthit.gov/topic/security-risk-assessment-tool
- Industry Resource: https://www.hipaajournal.com/

SOX... SOC... SOC2

TL;DR THAT TLA

- Sarbanes-Oxley Act passed on July 30, 2002
- Reformed business financial practices in the wake of Enron and WorldCom
- Reduces corporate fraud and increases investor protections
- Criminal punishments to company officials for violations
- SOC1-4 are reporting standards that help you comply with compliance laws (including SOX, PCI, and GDPR)

SOX OBJECTIVES

Accuracy and reliability

Protect investors and the public

Processing integrity

Safeguards, privacy, and security

Prevent and detect errors

Segregation of duties

WHO IS IMPACTED

- Publicly-traded companies based in the U.S.
- Wholly owned subsidiaries of publicly traded companies
- International companies that have stocks or securities registered with the SEC
- Private companies in certain areas of financial reporting or providing certain services to publicly traded companies (SAS 70)
- Accounting firms that audit companies for SOX
- Private companies planning an initial public offering (IPO)

ROLES

Process Owners

- Solely responsible for owning a process that includes protected data
- Accountable for designing an effective and efficient process, using the right people and financial and technical resources
- The central point of contact for SOX compliance activities
- Involved in change management and/or project management

Internal Auditors

- Verify the financial statements of the company and the processes involved in creating them
- Review controls, policies, and procedures (Section 404 audit)
- Interview staff to confirm that their duties match their job description and that they have the required training to safely access financial information.

TYPES OF DATA

- Financial statements
  - Off-balance liabilities
  - Transactions
  - Obligations
- Structure of internal controls
- Drastic changes in financial position or operations
  - Acquisitions
  - Divestments
  - Major personnel departures

HOW TO COMPLY

- Establish an audit committee
- Define the scope using a risk assessment approach (within the bounds of budget and reason)
- Determine materiality and risks (Accounts, Statements, Locations, Processes, and Major Transactions)
- Identify SOX controls
- Perform a fraud risk assessment
- Manage process and control documentation
- Test key controls
- Assess deficiencies
- Deliver management's report on controls

IT RESPONSIBILITIES

- Access
  - Physical controls and electronic controls
  - Privileged access management with a least-privilege model (only access necessary to do the job)
  - Prevent tampering
- Security
  - Identify sensitive data
  - Monitor who and how it is being accessed
  - Detect, prevent, and respond to security incidents
  - Track data breach attempts and remediation efforts
- Data backup
  - Back up data and key systems
  - Minimize disruptions and data loss
  - Safeguard both original and backups
- Change management
  - Process established and followed for
    - Adding and maintaining users
    - Installing new software
    - Making changes to databases or applications that interact with financial data
  - Record and monitor systems for changes, log, and detect abnormalities
  - Demonstrate compliance in 90-day cycles

TYPES OF AUDITS

- Internal controls
- Network activity
- Database activity
- Login activity (success and failures)
- Account activity
- User activity
- Information Access

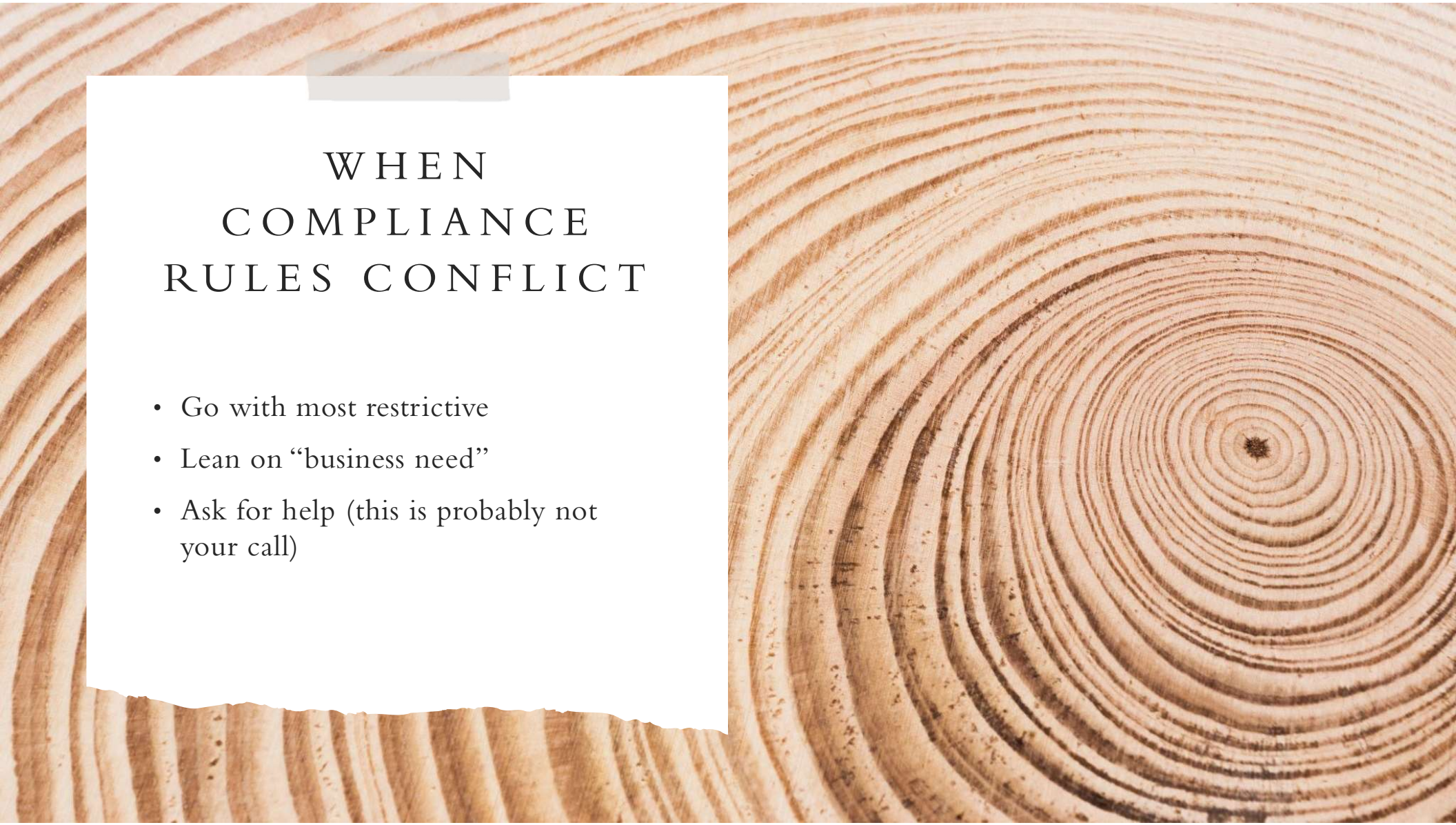
RESOURCES

- Full text of the Law: https://www.congress.gov/bill/107th-congress/house-bill/3763
- SOX Compliance Helpful Blogs:
  - https://www.varonis.com/blog/sox-compliance
  - https://www.upguard.com/blog/sox-compliance
  - https://www.investopedia.com/ask/answers/052815/what-impact-did-sarbanesoxley-act-have-corporate-governance-united-states.asp
  - https://corporatefinanceinstitute.com/resources/economics/sarbanes-oxley-act/
  - https://www.thebalancemoney.com/sarbanes-oxley-act-and-the-enron-scandal-393497
  - https://www.auditboard.com/blog/sox-compliance/
- SOC Reports Helpful Blogs
  - https://secureframe.com/blog/soc-1-vs-soc-2
  - https://bridgepointconsulting.com/insights/soc-reports-types-audit-meaning-questions

ZOOMING OUT

COMMONALITIES ACROSS REGULATIONS

- Clearly understand the business need for protected data
- Reduce data gathered to least necessary for business need
- De-identify, isolate, encrypt, and store data securely
- Limit access to data to only those who require it as part of their job responsibilities
- Basic internet safety
- Basic HR policies and training



WHEN COMPLIANCE RULES CONFLICT

- Go with most restrictive
- Lean on “business need”
- Ask for help (this is probably not your call)

QUESTIONS

Jennie.ocken.org jennie@ocken.org @jennieocken

QUESTIONS

Jennie.ocken.org jennie@ocken.org @jennieocken