Corporate Data Privacy in a Very Public World

Kimberly Akre, Engagement Director

CliftonLarsonAllen

cliftonlarsonallen.com

Is nothing truly private anymore?

Why does Data Privacy matter?

Because data is THE asset of the 21st Century

Privacy Myths

- Consumers don’t understand privacy and don’t think it is important
  - Customers routinely abandon shopping carts on websites because of demand for too much information
- Organization need unrestricted access to personal information in order to market to individuals, providing “consumer benefits”
  - Relationship marketing losing effectiveness, while permission marketing is growing
  - Lack of privacy protections put customer data at risk of exploitation
  - Data sharing benefits the date holder, but does it actually benefit the customer?
- Privacy value can only be measured in monetary cost and benefits.
  - Estimates of retail sales lost due to privacy concerns - $18 billion
  - Loss of business stature
  - Business are spending time & money responding to subpoenas for their compilations of personal data

Privacy Risks

- Data Breach Loss
  - High profile breaches – Target, Home Depot, Nieman Markus, Michaels, JP Morgan, Jimmy Johns, the NSA, etc.
  - Lawmakers and consumers are making noise now
  - Investigation by the FBI; legal action by the FTC and individual States
- Unexpected Costs
  - Forensic investigation
  - Breach response
  - Customer maintenance
  - Customer loss
- Customer Loss
  - Insecurity/Lack of trust

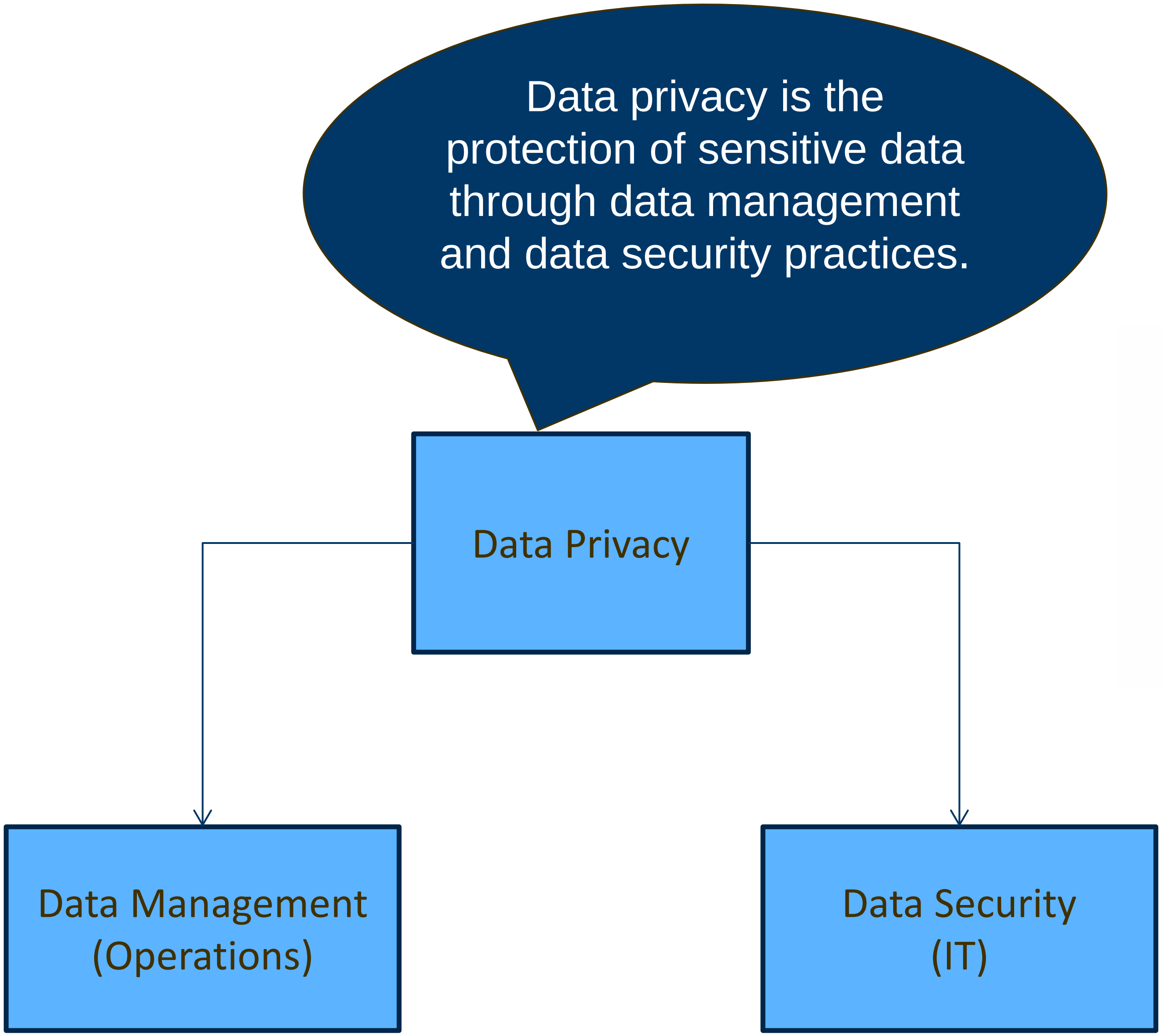
In making Data Privacy a priority, we show…

- ❖ Respect for individuals
  - Golden Rule
- ❖ Trust
  - If our clients don’t trust us, they will not be part of helping us grow
- ❖ Brand and Reputational Safeguarding
  - “Everybody has breaches these days….”

The FTC's Three Basic Principles of Privacy

- Privacy by Design
  - Build in privacy protections from the beginning, not as an afterthought
    - Limit the collection of data to the minimum necessary
    - De-identify the date you do collect, if possible
- Increased Transparency
  - Make privacy policies easy to read and understand
  - Make sure any claims about how you collect, use, or share data are truthful and complete
- Usable Choice
  - The choices you provide to consumers must cover all of your tracking practices, not just a subset
  - Be thoughtful about using sensitive data for marketing purposes; make it an opt-in choice for consumers

So, What is Data Privacy?



Data privacy is the protection of sensitive data through data management and data security practices.

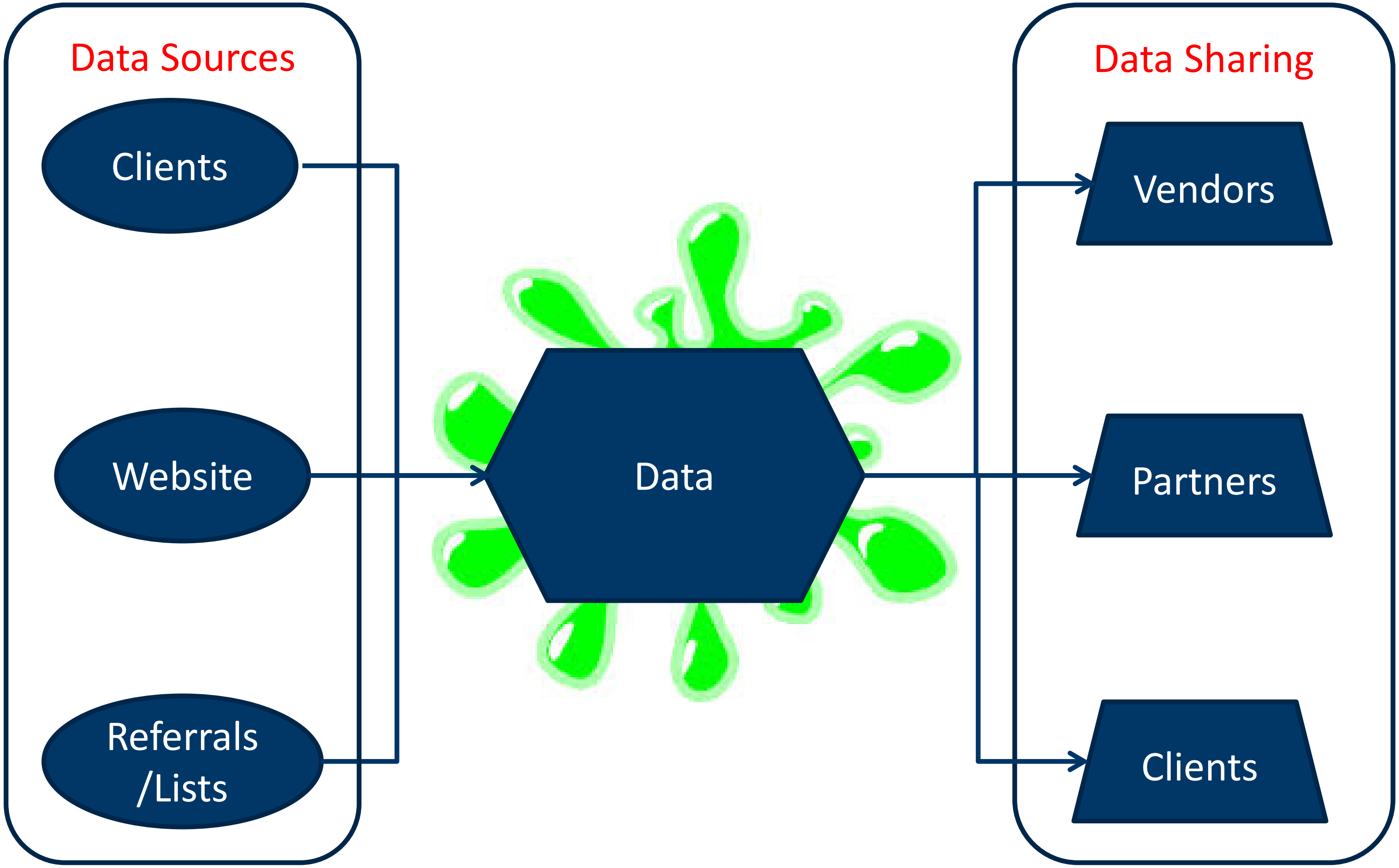
Data Privacy

Data Management (Operations)

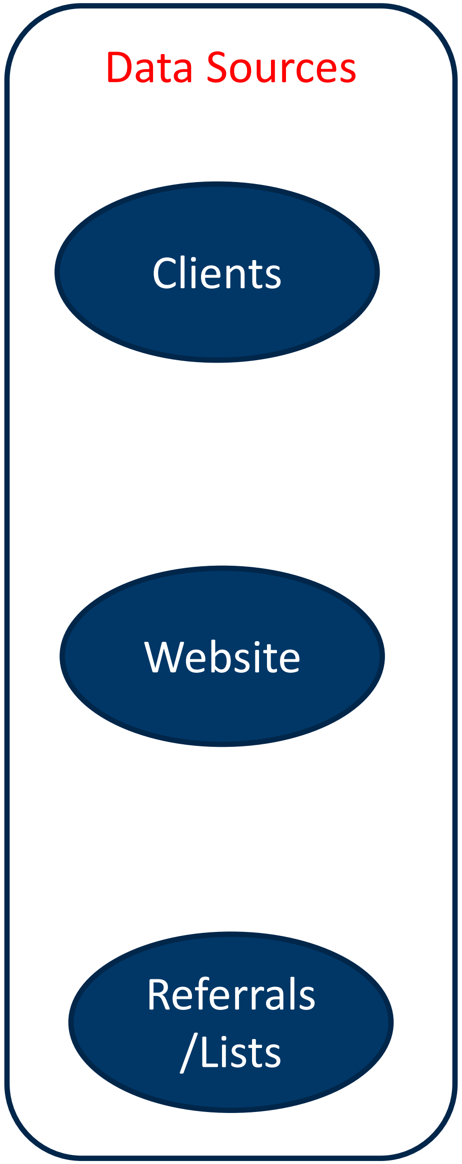
Data Security (IT)

Key Steps for Data Privacy

1. Know your Data Flow



Let’s Talk About Data Gathering



Data Sources

Clients

Website

Referrals /Lists

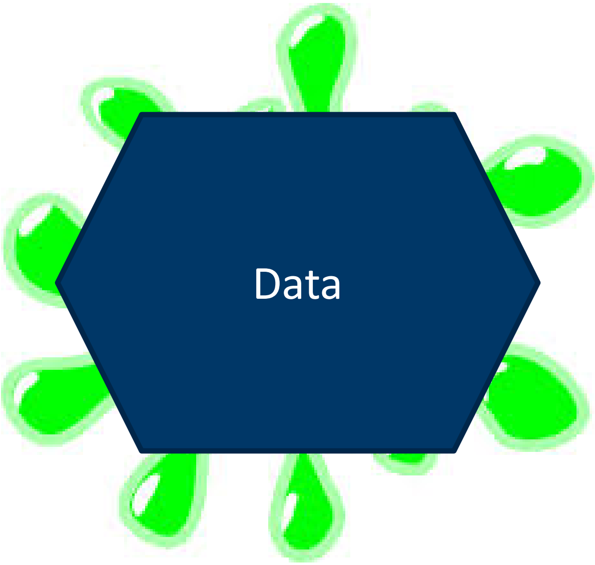
Where does data come from?

What promises were made implicit/explicit about data privacy/protection when the data was collected?

Are we collecting the data we need?
Are we collecting more data than we need?

Are we classifying the data correctly?

Let’s Talk About Data Storing



What are the legal / regulatory requirements for sensitive data security?

Where is sensitive data stored? Electronically? Paper?

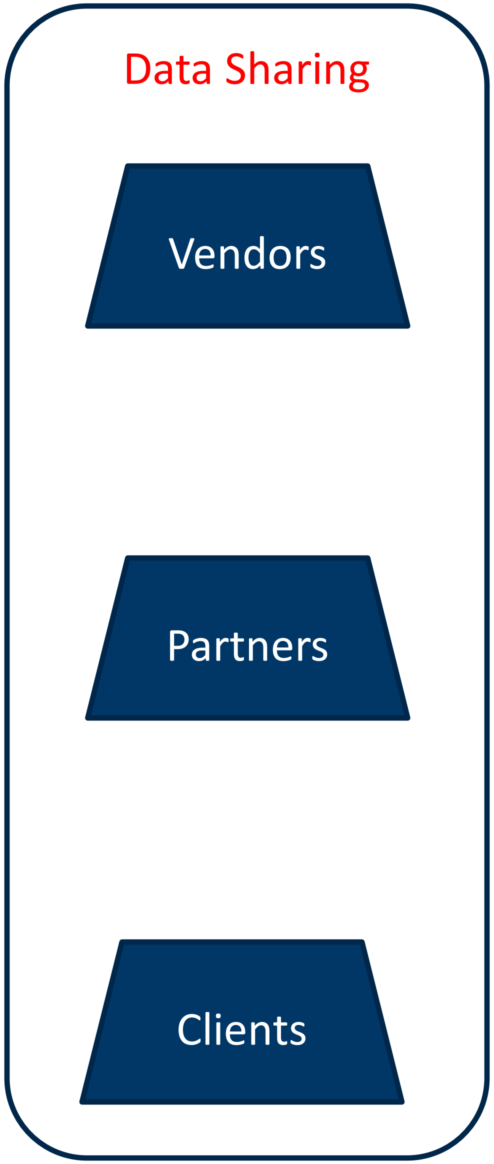
How is sensitive data secured?

How is access to sensitive data limited?

Are we securely disposing of data we no longer need?

Are we controlling data replication?

Let’s Talk About Data Sharing



Are we conscientious about what we share?

Is data sharing protected by a written agreement (contract including data privacy and security requirements; NDA, etc.)?

Are we performing due diligence on entities with whom we share sensitive data?

Are recipients aware of their responsibilities for privacy and security?

2. Know the Laws / Requirements for Protection of Sensitive Data

1. What is Sensitive Data?
   - PII (varies by state,) health data, financial data
   - Regulatory and legal definitions
   - Proprietary business information
2. Create and maintain a Data Classification Matrix
   - Classify data by types (Confidential, Secured, Public, etc.)
   - Define security requirements, access and retention periods by classification
3. Be ready to address a data breach

3. Define and Maintain Your Process

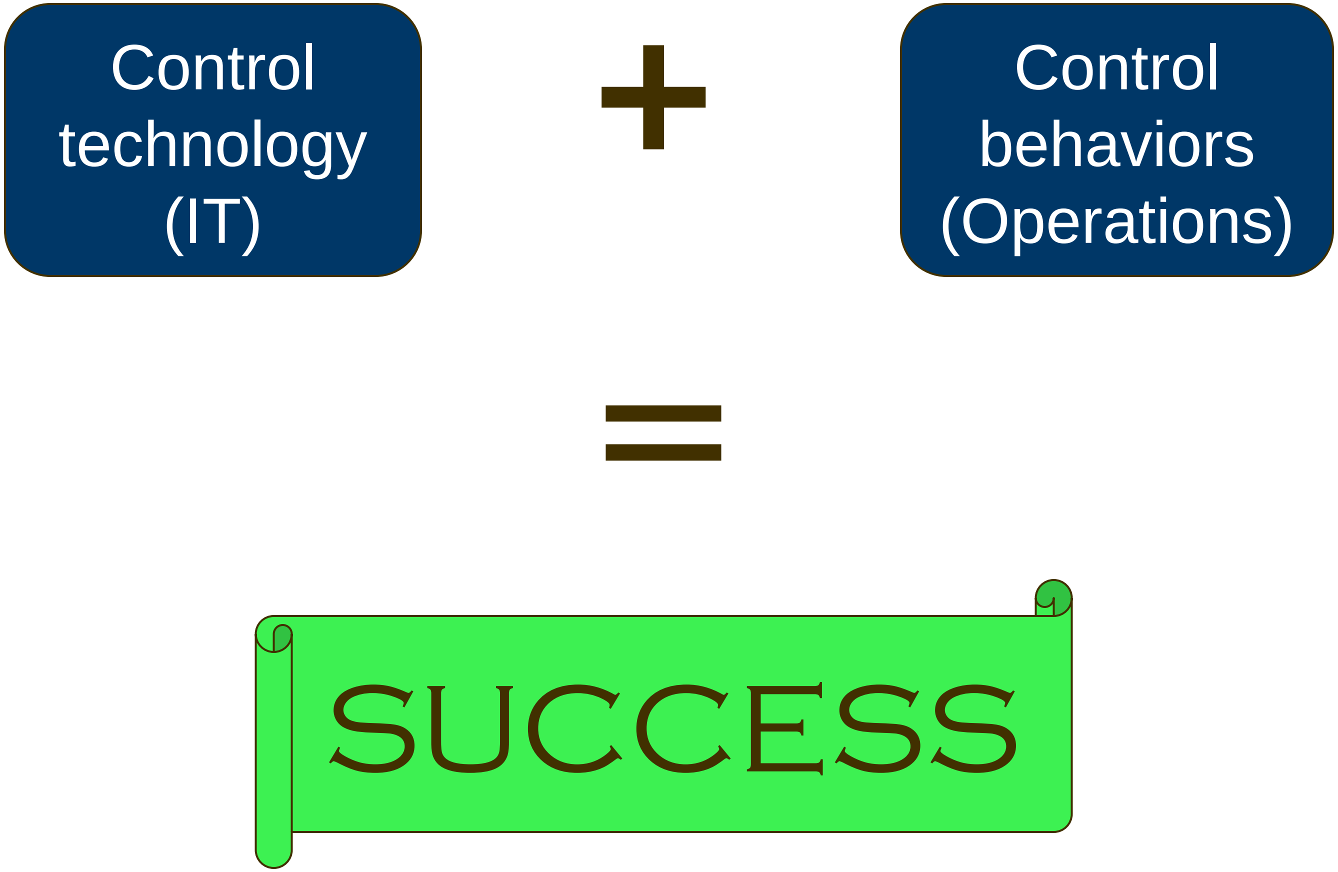
1. Define processes for data collection, storage, sharing, access, and destruction (& follow them!)
   - Assign a data custodian
2. Prevent sensitive data replication
   - Reports
   - Email
   - Local hard drives

3. Perform annual maintenance on your program
   - Retrain staff members on their responsibilities
   - Review the data privacy program and all components

Three Key Data Privacy Principles

1. Know your data flow
    1. Where did it originate?
    2. Where is it shared and with whom?
    3. Who owns the data?
2. Know the laws/requirements to protect key data
    1. Assign a data custodian
3. Define and maintain your process
    1. Do not replicate data
    2. Train your staff
    3. Review your program

For a Data Privacy Program to succeed…



Control technology (IT)

+

Control behaviors (Operations)

=

SUCCESS

Kimberly Akre, CISA, CIPP/US, PCI-QSA
Engagement Director
Kimberly.Akre@CLAconnect.com
612-397-3225

CliftonLarsonAllen

cliftonlarsonallen.com

twitter.com/
CLA_CPAs

facebook.com/
cliftonlarsonallen

linkedin.com/company/
cliftonlarsonallen