SQUIRE PATTON BOGGS

Data Privacy for Non-Profits: A Toolkit for Sound Stewardship

Petrina A. McDaniel

State Bar of Georgia
ICLE | 15th Annual Nonprofit Law Seminar
March 8, 2018

Agenda overview:

SQUIRE PATTON BOGGS

- **Section 1: Why Data Privacy Should Matter to Non-Profits**
- **Section 2: A Closer Look at Specific Laws Affecting Non-Profits**
- **Section 3: Better Safe than Sorry—Preparing for a Possible Breach**
- **Section 4: Privacy Practice Pointers**
- **Section 5: Q&A**

SQUIRE PATTON BOGGS

Section 1:
We're a Non-Profit—Why Does Data Privacy Matter?

Importance of Data Privacy

SQUIRE PATTON BOGGS

- **Privacy** is all about **people** and underpins most organizations and business processes (whether non-profit or for-profit).
- Non-profits collect and manage wide-ranging **personally identifiable information ("PII")** through various activities.
- Hackers are not the only threat. The most common risks can arise in everyday activities that lead to ***unintentional privacy breaches***:
  - **Conducting e-commerce on a website**, such as processing payments or event registrations online
  - **Storing and transferring PII** about employees, volunteers, donors, and other individuals
  - **Allowing partners or vendors to access PII** without safeguards
  - **Storing PII on cloud servers or systems or allowing access to PII on laptops and smartphones** without safeguards

Importance of Data Privacy

SQUIRE PATTON BOGGS

- Collection and use of PII comes with costly risks.
- For non-profits, failure to protect data privacy can lead to:
  - ***Operational losses***
    - Time and money spent investigating, communicating with third parties and any government or agency officials (or defending litigation), handling any related public relations or media issues
    - Potential organizational shutdown of electronic systems
  - ***Reputational harm***
    - Loss of public trust and potentially the loss of donor and vendor relationships

Privacy Landscape in the US (in one slide!)

SQUIRE PATTON BOGGS

- The US does not have a single, comprehensive federal law regulating privacy and the collection, use, processing, disclosure, and security of PII.
  - Instead, there is a patchwork of laws governing privacy and PII:
    - System of federal rules that are sector-specific: (COPPA, GLBA, HIPAA, TCPA, FCRA, FERPA, etc.)
    - System of state laws (i.e., data breach notifications laws)
    - Government regulators (FCC, FTC, State AGs – “unfair or deceptive practices”)
    - Common law principles (invasion of privacy, negligence, etc.)
    - Industry self-regulation (i.e., regulations that do not have the force of law but are considered best practices)
- Other considerations include contracts with clients/constituents and vendors
- Privacy policies, terms of use, and other online representations

What is PII?

SQUIRE PATTON BOGGS

Non-profits often collect and store sensitive personal information that is protected by law as confidential. ***The first step is knowing what is considered confidential and sensitive information****.*

Question for the audience: Which of the following are protected under the law as personally identifiable information?

a. Date of birth
b. Fingerprint
c. Social security number
d. Bank account information

PII Explained

SQUIRE PATTON BOGGS

Answer: ALL OF THE ABOVE. **Sometimes, with one caveat*:

- PII is typically defined and varies by each statute, but generally under state data breach statutes includes a **first** and **last name** of an individual **AND** other identifying information that can be used to identify, contact, or locate a single living person, or to identify an individual in context.
- Examples include email addresses/passwords, social security and driver's license numbers, biometric data, and medical or financial information.
- Generally **does not** include city or state of residence, zip code, area code, gender, age, or aggregate data that cannot be broken down to identify a specific individual.
- PII does not include publicly-available information.

SQUIRE PATTON BOGGS

Section 2: A Closer Look at Specific Laws Affecting Non-Profits

No IRS Rule for Non-Profits' Data Privacy Practices

SQUIRE PATTON BOGGS

IRS is the primary regulator for non-profits, but there are not any applicable requirements on this issue from the IRS.

- IRS Pub. 1075 - cybersecurity rules for *tax preparers*
  - IRS defined **encryption requirements and provided recommendations to agencies on how they can comply with the requirements in various scenarios**, *i.e.*, remote access, email, data transfers, mobile devices and media, databases, and applications.
- The only likely consequence for violating IRS rules would be losing exempt status – ***extremely unlikely to result from a cyber issue as far as we have seen.***

State AGs, not FTC, Regulate Privacy-Related Activity

SQUIRE PATTON BOGGS

- **The FTC usually refrains from pursuing enforcement actions against non-profits** under Section 501(c)(3) of the Internal Revenue Code because these entities carry on business in *pursuit of their tax-exempt purposes rather than for their own profit or that of their members.*
  - **Section 5 of the FTC Act regulates privacy/cyber actions to protect consumers from "unfair and deceptive trade [security/privacy] practices": No current §5(a) jurisdiction over non-profits**
  - ***Exception**: FTC may exercise jurisdiction if it believes that a non-profit organization is using charitable assets for the personal benefit of its officers, directors, employees, or other insiders, when it believes an organization's business primarily benefits private pecuniary interests (such as those of a for-profit fundraiser), or when it believes an organization's tax-exempt status is a sham.*
- All 50 states have "mini FTC acts" that ban "unfair and deceptive" practices targeted at consumers.
  - **State laws apply to non-profits, and state AGs can exercise power over non-profits for privacy violations.**

PCI Data Security Standard – The Global Data Security Standard

SQUIRE PATTON BOGGS

- **PCI Data Security Standard ("PCI DSS")** calls for certain technical and operational systems when handling major credit cards and imposes fines and fees for non-compliance.
  - **12 security standards created by the credit card industry**
  - **Intended to protect cardholder data; critical requirement in vendor contracts**
- Standard requires all entities processing credit card payments to erect an array of security controls, including firewalls, access controls, monitoring, and encryption of cardholder data during transmission and storage.

TIP: *In the event of a lawsuit following a breach, PCI compliance may be a strong argument that the merchant was not negligent with consumer data. *However, PCI compliance does not mean that a company is immune from governmental investigations or civil suits based upon a breach.*

PCI Data Security Standard

SQUIRE PATTON BOGGS

- **PCI DSS compliance consists of common sense steps that mirror security best practices.**

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Telemarketing Sales Rule for Non-Profits

SQUIRE PATTON BOGGS

- ***Does your organization use telemarketing/third-party companies to solicit contributions?***
- FTC's Telemarketing Sales Rule applies to interstate calls made by **for-profit telemarketers to solicit charitable contributions**.
  - Requires that telemarketers:
    - Disclose if purpose of the call is to ask for a donation
    - Disclose the name of the charity or organization
    - Maintain an internal do-not-call list for those who ask not to be called again
    - Maintain records for two years
    - Have an opt-out option for individuals on any robocalls
  - Prohibits telemarketers from:
    - Making false or misleading statements to induce a contribution
    - Making calls by autodialer or with prerecorded messages unless the person is a current member or has donated in the past
    - Making calls before 8 am or after 9 pm

When Non-Profit Telemarketing Goes Wrong…

SQUIRE PATTON BOGGS

- InfoCision, a for-profit telemarketer based in Ohio, places millions of calls to consumers on behalf of hundreds of charities.
- According to the FTC complaint, InfoCision began the calls with a “soft sell” by asking consumers to mail or hand-deliver materials from the charity to their family, friends, and neighbors.
- InfoCision did not immediately tell consumers that it was calling to ask for a charitable donation. Instead, it waited until the end of the call to ask consumers to make a contribution.
- The FTC complaint alleged that InfoCision violated the TSR by making false or misleading statements to induce a charitable contribution.
- In January 2018, InfoCision agreed to a $250,000 settlement with the FTC for these violations.

What did InfoCision do wrong?

What InfoCision Should Have Done…

At the beginning of each call, InfoCision should have clearly and promptly disclosed the name of the charity upon whose behalf it was calling and stated that the purpose of the call was to

ASK FOR A CONTRIBUTION.

The Telephone Consumer Protection Act (TCPA) and Non-Profits: Does it Apply?

SQUIRE PATTON BOGGS

- The TCPA generally requires prior express consent for calls made using an **autodialer** (i.e., automated technology) or with an artificial or prerecorded voice. Manual calling does not violate the TCPA.
- Text messages are equivalent to calls under the TCPA.
- **Non-profits are *generally deemed exempt** if the messages are *purely informational* and do not involve any telemarketing (i.e., advertising).** "Prior express written consent" is required for telemarketing calls.
- The scope depends on the type of number called:
  - If call is made to a residential number, **no prior consent is required** for prerecorded calls if purely for informational purpose or if made by or on behalf of a tax-exempt non-profit.
  - BUT if prerecorded call is made to wireless number, the **non-profit still needs prior express consent, whether written or oral, for the call**.

TIP: *Documentation of consent is key – written consent is always best.*

- **LIABILITY CAN BE SIGNIFICANT** ($500 per violation, up to $1500 for treble damages)

TCPA Compliance for Non-Profits: The Do Not Call Registry

SQUIRE PATTON BOGGS

- TCPA generally prohibits telemarketing/advertising calls to phone numbers on the National DNC Registry.
- Because of the limits to the FTC's authority, **the Registry does not apply to political calls or calls from non-profits and charities** (but the Registry does cover telemarketers calling on behalf of charities).
- This means that a non-profits can make calls asking for charitable donations without violating the DNC, but remember, any calls using automated technology to cell phones still requires some form of consent.

TIP: *If part of the call involves the sale of a product or service (even if part of the proceeds go to charity), DO NOT ASSUME the call is exempt from the TCPA. These calls may be considered "dual purpose," which is the equivalent of a telemarketing call, and the exemption will not apply. Instead, the charity would need to show "prior express written consent" for each call.*

TCPA Compliance Pointers for Non-Profits

SQUIRE PATTON BOGGS

- If using telemarketers or automated technology to reach your donors, volunteers, or constituents, remember to:
  - Identify the organization name and telephone number in any prerecorded message or autodialer calls;
  - Include an opt-out in any call made by artificial or prerecorded voice;
  - Beware of co-venture campaigns where calls made for both telemarketing and charitable purposes may trigger general TCPA rules; and
  - Remember, informational (non-advertising) calls made to cell phones using automated technology also require some form of consent (written or oral); and
  - Maintain an internal do-not-call list for individuals who expressly ask not to be called.

Data Storage State Laws You Should Know…

SQUIRE PATTON BOGGS

In addition to federal regulations, **state laws add another level of compliance**:

- California Civil Code: "A business that owns or licenses personal information about a California resident **shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information**…." Consumers injured by a violation may file civil actions for a violation of this requirement.

Massachusetts, Oregon, Rhode Island, and Nevada enacted strong privacy regulations, including certain data encryption requirements.

- **Massachusetts, Oregon, and Rhode Island**: Businesses that own license, store, or maintain personal information of a state resident must **implement a written information security program and implement certain system security measures**, including encryption of personal information during transmission (to the "extent technically feasible") and when stored on laptops and other portable devices.
  - Enforcement in Massachusetts and Rhode Island by the AG
  - Enforcement in Oregon by the Director of the Department of Consumer and Business Services with civil actions impliedly permitted where damages result from violation
  - ***Third party vendors**: The Massachusetts regulations require covered entities that retain outside service providers to include in the written contract a requirement that the vendor implement and maintain appropriate security measures to comply with the data security regulations.*
- **Nevada** (Nev. Rev. Stat. § 603A.215): **Requires businesses accepting payment cards to follow PCI DSS** and requires all others "doing business in this State" to encrypt all customer personal information (other than facsimiles) that is electronically transmitted "outside of the secure system of the data collector."
  - Enforcement by the AG or DA

Data Storage State Laws You Should Know…

SQUIRE PATTON BOGGS

Under **Georgia law**, businesses discarding business records that contain personal information must:

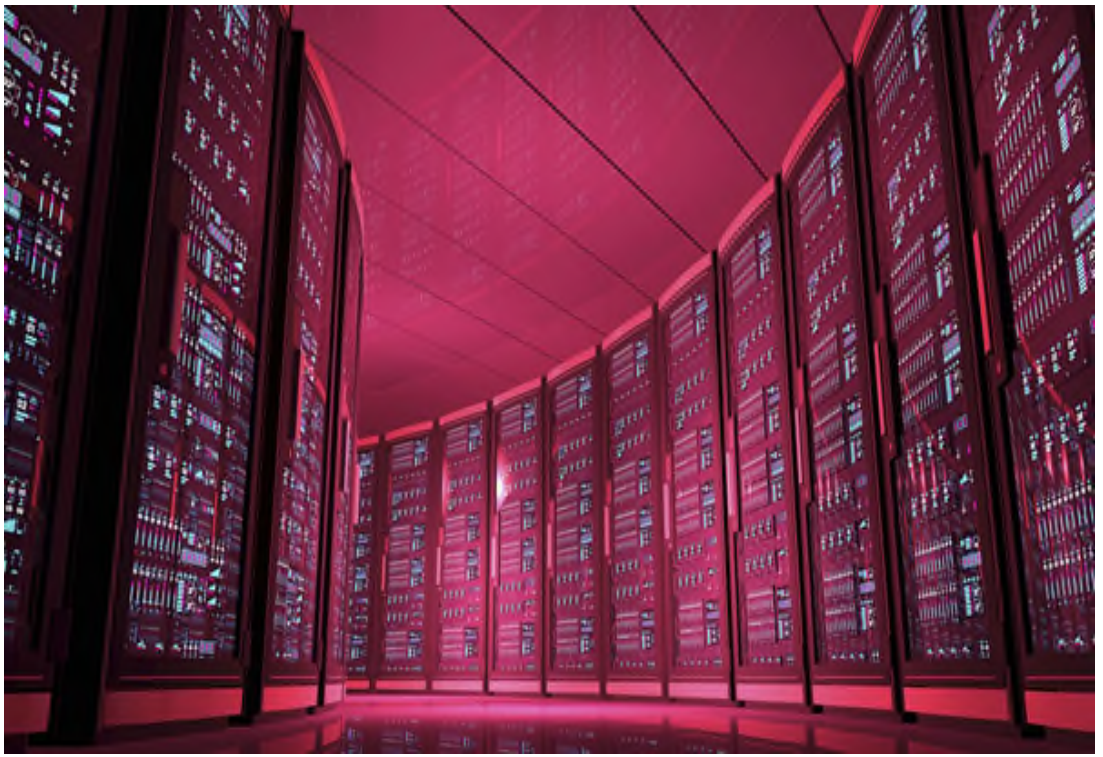
- Shred the customer's records;
- Erase any personal information in the record;
- Modify the record to be unreadable; or
- Take actions it "reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the customer's record for the period between the record's disposal and the record's destruction"

O.C.G.A. § 10-15-2. Investigation and enforcement of violations of this provision are handled by the AG.

TIP**: Read and understand the state laws carefully. Some state regulations do not only apply to businesses operating in that state—**it applies if you have a single donor/constituent living there and you collect data from that person.

SQUIRE PATTON BOGGS

Section 3: Better Safe Than Sorry—Preparing for a Possible Breach



State Data Privacy Laws

SQUIRE PATTON BOGGS

- Question for the audience: How many states have passed laws requiring private or governmental entities to notify individuals of security breaches involving PII?
  a. 3
  b. 15
  c. 33
  d. 48

State Data Privacy Laws

SQUIRE PATTON BOGGS

- Increasing number of state cybersecurity laws
- **With the exception of Alabama and South Dakota**, all states (and D.C., Guam, Puerto Rico, and the Virgin Islands) have passed data breach notification laws.
- *****However***: *On January 25, 2018, the South Dakota Senate approved the state's first data breach notification law. The proposed law is now in the South Dakota House of Representatives for consideration and, if approved, will be sent to the Governor to be signed into law.*
- ***AND***: *On March 1, 2018, the Alabama State Senate passed the Alabama Data Breach Notification Act, which will require private companies and state agencies to report data breaches to affected consumers. The measure was approved by a 24-0 vote. Bill is now in the House of Representatives.*
- These breach laws generally cover:
  - Who must comply with the law;
  - What constitutes "personal information";
  - What constitutes a breach (e.g., unauthorized acquisition of data);
  - What is required to give notice of breach (e.g., timing and method); and
  - Whether there are exemptions, such as for encrypted information, and risk of harm.

State Data Privacy Laws

SQUIRE PATTON BOGGS

- Many statutes provide that if covered entities are compliant under **HIPAA** or **GLBA** for security breach procedures and data breach notification, compliance under the state statute is also satisfied.
- **Trend of expanding the definition of "personal information"**
- **Some statutes provide for private right of actions; others do not and permit only the state AG to bring enforcement actions**
- ***TIP on Third-Party Vendors:*** *Even if a vendor causes a data breach, it is ultimately the organization's responsibility to notify its customers. In the aftermath, if affected consumers bring litigation, they will likely sue the company (and possibly the vendor), and it will be the company's reputation and brand that will be most affected.*

Preparing for a Breach

SQUIRE PATTON BOGGS

1. Know your current practices.
2. Assess risks.
3. Implement best practices for your organization.

Know Your Current Practices

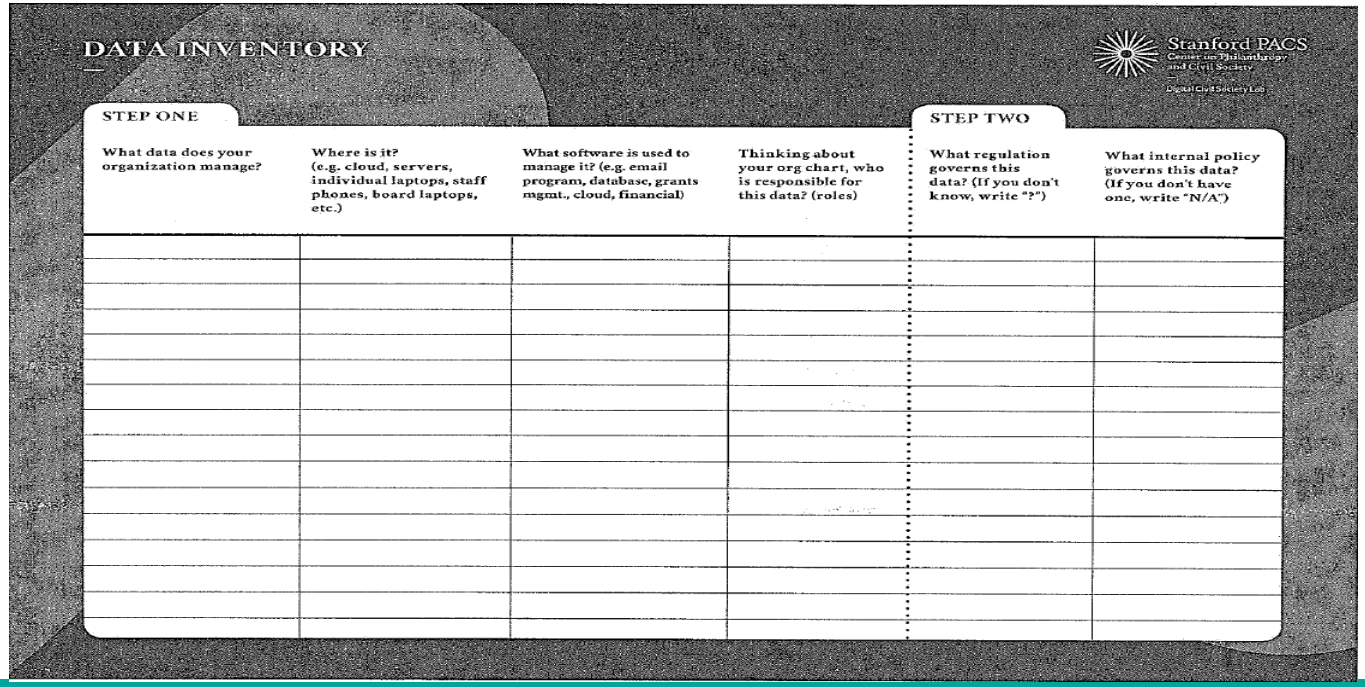
SQUIRE PATTON BOGGS

- Determine what privacy policies and procedures are in place for (1) collection; (2) use; (3) securing; (4) sharing; and (5) disposal of PII.
- **Are the practices followed?**
  - Discuss actual practices with IT, HR, and legal
  - Review vendor contracts, physical security, any outsourced functions, third-party hosting vendors, IT help desk management, and internal policies and procedures

TIP: *Consider assembling a "Privacy Committee" to establish buy-in and commitment from other functional groups. Although it is critical that one person (or group) "owns" privacy in an organization (and everyone is aware of the ownership), it is important to include others to ensure organizational buy-in to gain perspective on what privacy means within other functional departments within the organization.*

Develop a (Realistic) Incident Response Plan!

- An IRP does not have to be 100 pages – make it simple, practical, and functional.
- Begin the process with a privacy assessment to understand how your organization collects, uses, secures, shares, and disposes PII
- The Nonprofit Technology Network offers a free template assessment tool on its website, www.councilofnonprofits.org
- Digital Impact offers a one-pager that can serve as an inventory tool:



DATA INVENTORY

Stanford PACS
Center on Philanthropy and Civil Society

STEP ONE				STEP TWO	
What data does your organization manage?	Where is it? (e.g. cloud, servers, individual laptops, staff phones, board laptops, etc.)	What software is used to manage it? (e.g. email program, database, grants mgmt., cloud, financial)	Thinking about your org chart, who is responsible for this data? (roles)	What regulation governs this data? (If you don't know, write "?")	What internal policy governs this data? (If you don't have one, write "N/A")

What Should Be in the Plan?

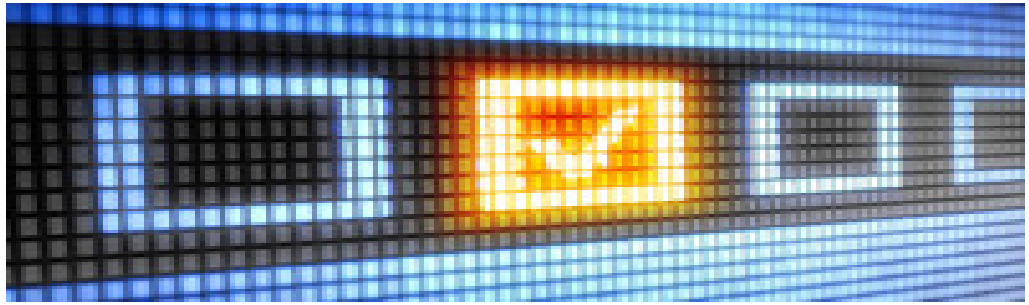
SQUIRE PATTON BOGGS

- Purpose
- Roles and responsibilities
- Escalation procedures
- Types of incidents
- Incident-specific procedures (i.e., process for engaging counsel, forensics vendors, ransomware vendors, etc.)
- Communications plan (PR/media communications)
- Contact information (include multiple numbers and representatives from HR, GC, IT, communications, etc.)

Work the Plan

SQUIRE PATTON BOGGS

- Response plan “cheat sheets” organized by role
- Proper training for team members
- Vendors engaged through counsel
- Privilege protocol established
- Establish pre-existing relationships with law enforcement
- Tabletop/security drills
- Continually revise and adapt plans and protocols based on changing needs or organization



Update Written Policies and Guidelines

SQUIRE PATTON BOGGS

- **Employee Personal Information Policy:** internal-facing policy for the protection of PII and information assets; can be incorporated into an employee handbook or a code of conduct
- **BYOD ("Bring Your Own Device" to Work) Policy:** governs the use of smartphones, tablets, and other mobile devices to perform work, both at the office and during nonworking hours
- **IT Resources and Communications Policy:** addresses the use of all company IT resources and communications systems
- **Password Protection Policy:** establishes a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change
- **Document Retention Policy:** establishes and describes how a company expects its employees to manage company data from creation through destruction
- **Vendor Due Diligence Policy/Checklist:** requires vendor due diligence before any engagement, and **should include standard contract terms that support the organization's privacy and information security programs; ensures regular vendor oversight and contract enforcement**

SQUIRE PATTON BOGGS

Section 4:
Privacy Practice Pointers

Promote Awareness Organization-Wide

SQUIRE PATTON BOGGS

- **Train staff and employees regularly:** an annual privacy training program is key to keeping information (and processes) fresh.

TIP: *When a significant privacy event happens in the news, take the opportunity to explain what happened to employees and staff, and offer a "lesson learned" practice pointer.*

Think Ashley Madison breach, Equifax breach, Wannacry Ransomware attack, etc.

- **Role-play:** In addition to table top drills, keep the organization on its toes by sending out fake emails that illustrate a phishing, social engineering, or ransomware attempt. ***Tax season is prime time for these attacks to occur.***
- **Develop standard privacy impact/incident forms that employees can fill out as the need arises.** Have an open-door policy and offer to assist with completion of the forms if an incident occurs.
- **Use your good work to your advantage!** Even if grant applications do not ask for information related to privacy/security measures of the organization, volunteer this information to show that the organization takes privacy and data security seriously.

Insurance Considerations

SQUIRE PATTON BOGGS

- Consider purchasing cyber insurance for the organization and requiring vendors to name organization as **an additional insured on policy**.
- **Your organization will be liable in the event of a vendor breach of your employee or constituent PII.**
- **What are the benefits? Insurance will cover notification costs, IT forensics costs, public relations, credit monitoring, defense costs in litigation or regulatory actions, and other services.**
- Interview several brokers to discuss the **appropriate amount of coverage** based on size and complexity of organization and vendor relationships.

Practical Data Privacy Tips To Do *Today*!

SQUIRE PATTON BOGGS

- **Determine what cyber and privacy policies and procedures you have. These questions will help you determine what is missing and whether policies are being followed:**
  - Do we have an information security program or policy? If so, does our program align with an industry standard? If so, which one? (i.e., NIST)
  - Do we have privacy policies in place to address internal handling of PII and security protocols?
  - Do we conduct annual privacy/security awareness training, document attendance, and enforce requirement?
  - Have we designated at least one individual responsible for cybersecurity?
  - Do we have 2-factor authentication for remote access and internal administrative access?
  - Do we encrypt laptops and USB drives?
  - Do we conduct regular software updates/patches?
  - Do we have a vendor management program?

More Questions To Ask!

SQUIRE PATTON BOGGS

- How long do we store security and event logs? Do we review them? If so how often?
- How often do we audit account permissions? Do we have a process for requesting higher permissions?
- Do we have logging enabled on our email and file servers, etc.?
- Can we add “EXT” to incoming emails from external domains?
- Are you notified when someone changes job function or authority? Do you notify IT? How soon?
- Who do you notify when an employee departs? How soon?
- For employee records stored on company servers, is access restricted to HR only as needed?
- What is the process for handling information security incident responses?
- What security/privacy training do new employees receive?

Bringing it All Together

SQUIRE PATTON BOGGS

Advance planning (a) lessens the likelihood of a data security breach, (b) limits the liability and exposure in the event of a data loss, and (c) represents good stewardship of your organization.

- ***Recommended Steps***:
  - Understand the landscape of relevant laws that apply to your organization (and consult counsel to understand how to comply with them)
  - Assess and address current risks; create an incident response plan and relevant privacy policies; make sure to address any technological gaps (partner with IT)
  - Implement comprehensive employee training (including drills and table-top exercises)
  - Review current contracts and data security practices with third-party vendors to identify and address high-risk situations
  - Hire good help! Identify and engage external resources (counsel and forensic vendors) for ongoing advice and crisis response
  - Consider purchasing cybersecurity insurance

SQUIRE PATTON BOGGS

Section 5: Q&A

SQUIRE PATTON BOGGS

Download Today's Presentation

Data Privacy for Non-Profits: A Toolkit for Sound Stewardship

Available now at
https://www.squirepattonboggs.com/en/insights/events/2018/03/data-privacy-for-nonprofits-a-toolkit-for-sound-stewardship

Today's Presenter

Petrina A. McDaniel
Partner
+1 678 272 3207
petrina.mcdaniel@squirepb.com

Petrina McDaniel is a commercial litigator and Certified Information Privacy Professional (CIPP/US) whose practice uniquely blends complex litigation, regulatory compliance, and privacy counseling.

As a member of the firm's Litigation and Data Privacy & Cybersecurity practices, Petrina represents domestic and multinational companies across various industries, including telecommunications, aviation, insurance, retail, technology, healthcare and financial services, and has successfully litigated complex commercial cases in state and federal courts across the country, including appellate courts and administrative and arbitral forums.

Petrina has particular expertise in defense litigation under the Telephone Consumer Protection Act (TCPA), and regularly serves as lead counsel in individual and class action litigation across the country. Petrina's TCPA practice spans over a decade and clients look to her for creative ways to ensure compliance for their marketing strategies under the statute.

In addition to litigation, Petrina works with clients to protect the privacy and security of consumer information through the development and implementation of privacy compliance policies, information security programs, and data breach response protocols. She assists clients in protecting consumer information through risk management programs and by strengthening privacy and data security provisions in commercial agreements. In addition, Petrina counsels clients on data breach and incident response, including executing incident response plans, commencing remediation, and coordinating reporting obligations and regulatory responses.

Global Coverage

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Budapest
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Doha
Dubai
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Moscow
Newark
New York
Northern Virginia
Palo Alto
Paris
Perth
Phoenix
Prague
Riyadh
San Francisco
Santo Domingo
Seoul
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC
West Palm Beach

Africa
Argentina
Brazil
Chile
Colombia
Cuba
India
Israel
Italy
Mexico
Panamá
Peru
Turkey
Ukraine
Venezuela

Office locations
Regional desks and strategic alliances