Protecting the Information of…Clients, Donors, the Organization, Oh MY!

Stacey Keegan

November 14, 2012

PRO BONO™
PARTNERSHIP / ATLANTA

Mission of Pro Bono Partnership of Atlanta:

To maximize the impact of pro bono engagement by connecting a network of attorneys with nonprofits in need of free business legal services.

PRO BONO PARTNERSHIP/ATLANTA

Pro Bono Partnership of Atlanta Eligibility & Other Information

- In order to be a client of Pro Bono Partnership of Atlanta, an organization must:
  - ✓ Be a 501(c)(3) nonprofit organization.
  - ✓ Be located in or serve the greater Atlanta area.
  - ✓ Serve low-income or disadvantaged individuals.
  - ✓ Be unable to afford legal services.
- *Visit us on the web at* www.pbpatl.org
- Host free monthly webinars on legal topics for nonprofits
  - ✓ To view upcoming webinars or workshops, visit the Workshops Page on our website

PRO BONO™
PARTNERSHIP / ATLANTA

Agenda

- Why Non-Profits Should Care About Data Privacy and Security
- Responsibilities and Risks of Collecting, Using, Securing, Sharing and Disposing of Personal Information
- How to Minimize Risks in 3 (Easy?) Steps
- Best Practices for Responding to a Data Breach
- Practical Privacy and Data Security Tips You Can Implement Today

PRO BONO™
PARTNERSHIP/ATLANTA

Why Non-Profits Should Care About Data Privacy and Security

- Non-profits may collect or have access to personal information about a lot of different people, including clients, volunteers, employees and donors
- This information can be used to better serve clients, manage volunteers and employees, and communicate with donors
- But the collection and use of personal information comes with certain risks and responsibilities

PRO BONO™
PARTNERSHIP/ATLANTA

What is Personal Information?

- Personal Information ("PI") is any information that can be used to uniquely identify an individual
- PI includes a person's name, address, phone #, DOB, email address, gender, race, etc.
- Sensitive Personal Information includes credit card numbers, financial account numbers, government issued ID numbers (driver's license, passport, military ID), social security numbers, and personal health information

PRO BONO™
PARTNERSHIP / ATLANTA

Responsibilities and Risks of Collecting, Using, Securing, Sharing or Disposing of PI

- Responsibilities
  - ✓ Legal and Regulatory Obligations
  - ✓ Contractual Obligations
  - ✓ Fiduciary Duty
- Risks
  - ✓ Regulatory or Legal Actions
  - ✓ Direct Financial Costs
  - ✓ Reputational Damage
  - ✓ Operational Losses

PRO BONO™
PARTNERSHIP / ATLANTA

There is not a single national omnibus privacy or data security law. Instead, the U.S. has developed a complex patchwork of privacy laws that vary depending on the nature and use of Personal Information.

Select U.S. Federal Laws

- Children's Online Privacy Protection Act
- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act
- Right to Financial Privacy Act
- Electronic Communications Privacy Act
- Computer Fraud and Abuse Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Info. Technology for Economic and Clinical Heath Act (HITECH)
- CAN-SPAM and Telemarketing Laws

Select U.S. State Law Issues

- Data Breach Notifications
- Identity Theft
- Use of Social Security Numbers
- Telephone/Fax Marketing
- Wiretapping or Recorded Phone Calls
- Employee Monitoring
- Computer Crimes
- Medical Privacy
- Financial Privacy
- Encryption and Data Security
- Records Disposal

PRO BONO™
PARTNERSHIP / ATLANTA

Related Webcasts

- Before You Swipe - Best Practices in Accepting Credit, Debit, and Pre-Paid Card Payments
  (Posted on March 22, 2012)
- Legal Issues of Social Networking
  (Posted on November 16, 2011)
- HIPAA Considerations for Small Nonprofits
  (Posted on July 20, 2011)
- Best Practices for a Legally Compliant Website
  (Posted on January 20, 2010)

PRO BONO™
PARTNERSHIP / ATLANTA

How to Minimize Risks When You Collect, Use, Share, Secure and Dispose of Personal Information in 3 (Easy?) Steps

PRO BONO™
PARTNERSHIP/ATLANTA

Step #1: Privacy Assessment

- How does your organization collect PI?
- How does your organization use PI?
- How does your organization secure PI?
- How does your organization share PI?
- How does your organization dispose of PI?

PRO BONO™
PARTNERSHIP / ATLANTA

How is Personal Information Collected?

- What is the method of collection?
  - ✓ Website
  - ✓ Paper Documents (employment applications, client intake forms, background checks, donation logs, etc.)
- Who is PI collected from?
- What kind of PI is collected?
  - ✓ Are you collecting Sensitive Personal Information?
  - ✓ Are you collecting too much? Too little?
- TIP: Only collect the minimum amount of PI that is necessary to perform a business function.

PRO BONO™
PARTNERSHIP / ATLANTA

How is Personal Information Used?

- How does your organization use PI?
  - ✓ To fulfill your mission?
  - ✓ For operational purposes?
  - ✓ For marketing purposes?
  - ✓ For fundraising purposes?
- Are you transparent about how you use PI?
  - ✓ Do you have a Privacy Policy? Are you compliant with it?
- TIP: Be sensitive and thoughtful about how and when you use PI. Give notice and obtain consent prior to using an individual's PI.

PRO BONO PARTNERSHIP/ATLANTA

How is Personal Information Secured?

- Where is PI stored?
  - ✓ Electronic Devices (computers, mobile devices, flash drives)? Are they encrypted?
  - ✓ Filing Cabinets or storage boxes? Are they on or off site?
- Who has access to it?
  - ✓ Employees, Volunteers, Board Members?
- How is it secured?
  - ✓ Are administrative, physical or technical safeguards used?
- TIP: Limit access to PI to only a few individuals who must use it to perform their job function

PRO BONO PARTNERSHIP/ATLANTA

How is Personal Information Shared?

- Do you share PI with third-parties (3Ps)? Why?
  - Example: The name and mailing address of everyone on your donor list is shared with the service provider you use to mail invitations to your next event.
  - Example: You swap mailing lists with another organization.
- If you share PI, what restrictions (if any) do you place on the 3P who receives your PI?
- How do you transfer PI between yourself and 3Ps?
- TIP: Via contract, always require 3Ps with whom you share PI to use such data only for its permitted purpose and to properly secure it.

PRO BONO™
PARTNERSHIP/ATLANTA

How Do You Dispose of Personal Information?

- What disposal method is used?
  - ✓ Do you shred paper documents containing PI?
  - ✓ Do you destroy or securely dispose of electronic equipment containing PI?
- How long do you keep PI?
  - ✓ Do you have a retention schedule for PI?
  - ✓ If PI must be retained for a long period of time, can it be securely archived or the PI redacted?
- TIP: Keep PI only as long as necessary to fulfill a business purpose. Once you no longer need it, securely destroy it.

PRO BONO™
PARTNERSHIP / ATLANTA

Step #2: Gap Analysis/Risk Assessment

- Based on the kind of PI you collect and your current privacy practices, determine which laws and regulations apply to your organization
- Conduct a gap analysis to determine steps you may need to take to close any compliance gaps
- Complete a risk assessment to determine if you are comfortable with your current practices or if you need or want to make changes
- Update policies and procedures accordingly

PRO BONO™
PARTNERSHIP/ATLANTA

Step #3: Implementation

- Implement and consistently apply administrative, physical and technical safeguards that are appropriate for the type of PI your organization collects
- Publish updated policies and guidelines
- Train data users on new policies and procedures

PRO BONO™
PARTNERSHIP / ATLANTA

Data Privacy and Security Safeguards

- ✓ Administrative
  - Have written information security and privacy policies
  - Promote awareness. Regularly train employees and volunteers.
  - Lead by example. Make privacy a priority.
- ✓ Physical
  - Keep paper documents containing PI in locked file cabinets
  - Shred paper documents and securely destroy/erase portable devices containing PI
  - Limit who has access to building keys or alarm codes
- ✓ Technical
  - Use anti-virus software and stay current with security patch updates
  - Use strong passwords. Passwords are like toothbrushes – everyone should have one, but you shouldn't share them!

PRO BONO™
PARTNERSHIP / ATLANTA

Best Practices for Responding to a Data Breach

- Don't Have One
  - ✓ Conduct a risk assessment
  - ✓ Perform a security audit
  - ✓ Create training programs
  - ✓ Promote privacy awareness
  - ✓ Implement policies
  - ✓ Manage your service providers

PRO BONO™
PARTNERSHIP/ATLANTA

Best Practices for Responding to a Data Breach

- Have a data breach response plan
  - ✓ Create a formal data breach response policy
  - ✓ Make it flexible enough to address a wide variety of incidents
  - ✓ Include protocols for internal breaches vs. third-party or vendor breaches
  - ✓ Identify an incident response team
    - Legal, IT, HR, PR, Board member(s), independent auditor

PRO BONO™
PARTNERSHIP / ATLANTA

Best Practices for Responding to a Data Breach

- Understand the scope of the breach
  - ✓ Determine where, what, who, when, why and how the information was compromised
  - ✓ Investigate immediately and thoroughly
  - ✓ Take all necessary and relevant actions to contain the breach and mitigate risks

PRO BONO™
PARTNERSHIP/ATLANTA

Best Practices for Responding to a Data Breach

- Determine which, if any, laws govern your next steps
  - ✓ Analyze all state data breach notification laws to determine relevancy
  - ✓ Is HIPPA implicated? PCI?
  - ✓ This analysis relies heavily on the due diligence done in the investigation stage to determine the scope of the breach

PRO BONO™
PARTNERSHIP/ATLANTA

Best Practices for Responding to a Data Breach

- Make appropriate notifications
  - ✓ Law enforcement
  - ✓ Breach Victims
  - ✓ State Attorneys General/Other state agencies
  - ✓ Special notification requirements for breaches implicating HIPPA or PCI
  - ✓ Credit Bureaus
  - ✓ Media
  - ✓ Notifications should be timely and thorough

PRO BONO™
PARTNERSHIP / ATLANTA

Best Practices for Responding to a Data Breach

- Conduct Post Breach Analysis
  - ✓ How well did you follow your incident response plan? What worked well? What can be improved?
  - ✓ How can a similar breach be prevented in the future? Review data security procedures
  - ✓ Monitor external response to breach notifications
  - ✓ Update policies and procedures
  - ✓ Update training program

PRO BONO™
PARTNERSHIP / ATLANTA

Practical Privacy and Data Security Tips You Can Implement Today

PRO BONO PARTNERSHIP/ATLANTA

Practical Privacy Tips You Can Implement Today

- Passwords – First Line of Defense
  - ✓ Make a password that is a minimum of 7 characters
  - ✓ Use a combination of upper case, lower case, and special characters, along with numbers
  - ✓ Make your password difficult to guess by trying one of the following examples:
    - Use a phrase such as #1Bravesf@n (Number 1 Braves Fan)
    - Use the first letters of a saying, sentence, or song lyric such as TmOtTbG! (Take me out to the ball game!)
  - ✓ Never use family names, your anniversary, or DOB
  - ✓ Never write passwords down on a sticky note

PRO BONO™
PARTNERSHIP/ATLANTA

Practical Privacy Tips
You Can Implement Today

- Email Usage
  - ✓ Do not send Sensitive Personal Information in unencrypted emails
  - ✓ Beware of email phishing schemes
  - ✓ Do not open, and delete immediately, suspicious emails containing unrequested attachments
- Portable Storage Devices
  - ✓ Do not save Sensitive Personal Information on flash or thumb drives. These are easily lost or stolen.

PRO BONO™
PARTNERSHIP/ATLANTA

Practical Privacy Tips
You Can Implement Today

- Clean Desk Policy
  - ✓ Do not leave paper documents containing PI in unsecured areas
  - ✓ Place files containing PI in locked filing cabinets and desk drawers. Do not leave the key in the lock.
  - ✓ Make sure you lock your workstation or computer before leaving it unattended. (Ctrl + Alt + Del)
- Report the loss, misuse or theft of PI promptly
  - ✓ Make sure data users know who to alert if this occurs

PRO BONO
PARTNERSHIP / ATLANTA

Practical Privacy Tips You Can Implement Today

- Beware of social engineering schemes.
  - ✓ Identity thieves may try to trick you into disclosing Sensitive Personal Information
  - ✓ Verify the identity and authority of anyone requesting Sensitive Personal Information
- Be careful when transmitting PI
  - ✓ Avoid leaving Sensitive Personal Information in voice mail messages
  - ✓ If you have to send PI via fax, confirm the accuracy of a number before you key it in. Arrange for and confirm prompt pick-up.

PRO BONO™
PARTNERSHIP / ATLANTA

For More Information:

If you would like more information about the services of Pro Bono Partnership of Atlanta, contact us at:

Phone: 404-407-5088

Fax: 404-853-8806

Info@pbpatl.org

www.pbpatl.org