Hendey, Leah

From: Amy Hawn Nelson <Amy.Hawn.Nelson@uncc.edu>
Sent: Tuesday, January 24, 2017 1:05 PM
To: Amy Hawn Nelson
Subject: Data Privacy and Security Tips

Dear Partners of the Institute for Social Capital,

"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

In honor of National Data Privacy Day on January 28th, we wanted to reach out to talk about Data Privacy and Security. We think there are some cost effective and easy ways to safeguard your agency's sensitive information, without the need for fancy computer costumes.

Some common data privacy risks

Storing and transferring data without clear data protection expectations in place.

- All data should be stored on a password protected computer or in a locked office. Passwords should have some complexity and be changed on a regular basis.
- **No information with personally identifiable information (ex. name, date of birth, address, etc.) should be emailed.** If information with PII must be transferred, we suggest other methods such as Dropbox, Google Drive, etc. When a file must be transferred, we encourage placing a password on the document and communicating the password by phone.
- Personal information should not be stored on smartphones or personal laptops.

Allowing unlimited access to data for employees and partners.

- Access should be limited to a need to know basis. Any access that is granted should have the ability to be audited.

Some simple tips:

If you collect it, protect it. There are many layers of security, and all are important.

- Legal (such as privacy notices and informed consent),
- Technical (access such as passwords, encryption, deidentification, etc.)
- Procedural (limit who is able to handle data, regular communication across all members of an organization around security, training around security, and clear protocols for a breach or incident),
- Physical (where data is stored whether electronic or hard copy)

Create a culture of privacy in your organization.

- Make data security a critical piece of staff training. When an incident occurs, it will likely happen because of human error or oversight, rather than a technical issue.
- Clearly communicate what is considered personally identifiable information (PII). This typically includes name, date of birth, SSN, Drivers License #, and any Acct # or Credit Card #.
- Require regular updates of software.
- Encrypt sensitive data.
- Have clear guidance in place regarding expectations around data security and hold annual trainings for all staff.

We hope this information is helpful as we all work to support data informed decision- making in our community. As always, we appreciate your partnership and your commitment to serving our community.

I also want to take this opportunity to let you know that I will be on maternity leave until May 2017. Ashley Williams Clark, ISC's Assistant Director will be ISC's Acting Director during this time. As most of you know Ashley, you know that ISC is in incredibly capable hands during this time.

If you have any questions or concerns, as always, please reach out to Ashley or Angelique Gaines.

We appreciate your continued partnership.

Best,

Amy Hawn Nelson, Ph.D.
Director of Social Research
UNC Charlotte | Urban Institute
Director, Institute for Social Capital, Inc.
9201 University City Blvd. | Charlotte, NC 28223
Phone: 704-687-1197 | Fax: 704-687-5327
amy.hawn.nelson@uncc.edu