PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

by Chris Castellano, VP of Information Technology

With increases in cyber-attacks, identity theft, and threats to personal information and security around the world, we wish to provide you with information about how ORC is working to safeguard the personal information of our clients, property owners and others who trust us with their personal information.

Generally, Personally Identifiable Information (PII) is any data that could potentially identify a specific individual. Non-public PII includes a first name, or initial, and last name plus one of the following: (i) social security number, (ii) driver's license number or state identification card number, (iii) financial account information (bank account number, credit card, etc.), or (iv) medical history. Companies that are trusted with any combination of this information are at risk for cyber-attacks, phishing, ransomware schemes, or more.

This risk is multiplied when storing or transmitting any of this information over the internet. To protect all those we serve, we strive to implement best practices and policies to protect our PII.

Specific requirements vary from state-to-state and are sometimes industry-specific. ORC has compiled a list of best practices from federal legislation and regulations, state statutes, federal handbooks, and other guidelines.

We recommend that all companies consider the following best practices for PII protection:

- Implement a written security plan for PII for employees to follow which should include at a minimum the following:
    - Collect PII only when necessary and authorized to accomplish the business mission.
    - Limit the use and communication of PII.
    - Develop a schedule for the regular review of the content, quantity, and security of PII.
    - **Do not electronically store or transmit any non-public PII over the internet without security controls or safeguards, such as encryption, to protect the confidentiality of such information.**
    - Properly and securely dispose or destroy PII in an appropriate and reasonable manner in accordance with any record retention or destruction requirements for your industry.

By implementing certain best practices, ORC is working to protect your organization and ours from exposing sensitive information and incurring the consequences that come from such exposure: lost funds, legal fees, public relations costs, cost of remediation, costs of services to affected customers, and more.

Specifically, email is a known exposure point regarding PII as many users simply fail to realize the default lack of security built into this communication channel. In light of this, ORC's policy is to avoid the transfer of PII over the internet by email attachments or in direct email correspondence. Our system monitors and scans all email for such content and acts on such messages. This means that you will find ORC employees relying on the simple use of secure alternate methods of file transfer for sensitive documents that contain PII instead of regular email. We hope that we can work with your organization to establish such successful transfer mechanisms, while advancing your project and protecting PII information.

We encourage discussion on how, using your tools or ours, we can assure protection of all personal information that we must share efficiently. At ORC, we are focused on the protection of PII. We would be happy to work with your agency or company to create a plan for transmittal of shared documents that will allow us to maintain security and protect privacy when sharing PII. ■■■