volunteermatters
Let's do something extraordinary

Our customers utilize Volunteers to attract and track volunteers. As a part of our management of volunteers we necessarily request and maintain personally identifiable information for those individuals. In some cases, this is to communicate with an individual that has an expressed interest in maintaining a relationship with our organization. In other cases it is to maintain compliance with internal policies, or government mandated regulations.

What is Personally Identifiable Information (PII)?
PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's
- license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Our Recommendation
Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission. The likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores.

All PII is not created equal. PII should be evaluated to determine its PII confidentiality impact level. The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. In general, we do NOT recommend maintaining high impact PII in your systems.

Examples of factors to be considered include:

- How easily PII can be used to identify specific individuals. For example, an SSN uniquely and directly identifies an individual, but a telephone area code identifies a set of people.
- How many individuals can be identified from the PII. Breaches of 25 records and 25 million records may have different impacts.
- Evaluation of the sensitivity of each individual PII data field. For example, an individual's SSN, driver's license number, or financial account number is generally more sensitive than an individual's phone number or ZIP code. Organizations should also evaluate the sensitivity of the PII data fields when the data from different fields is combined.
- Evaluation of the context of use of the PII. The context of use is the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. For example, the breach to a newsletter subscription list containing name, address, and phone number presents a lower potential risk than a list with similar data for undercover in law enforcement officers.
- Obligations to protect confidentiality. Organizations should consider their specific obligations to protect PII when determining the PII confidentiality impact level. Obligations to protect PII are specified in laws, regulations, and other mandates, including the Privacy Act and OMB guidance. Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal requirements to protect certain types of PII. For example, currently more than 25 states have adopted laws restricting or prohibiting the collection, use or disclosure of an individual's Social Security number.
- Access to and location of PII. Organizations may choose to take into consideration the nature of authorized access to and the location of PII. When PII is accessed more often or by more people and systems, or the PII is regularly transmitted or transported off-site, then there are more opportunities for the confidentiality of the PII to be compromised.

Social Security Numbers

As you may have implied from the above, the collection and storage of Social Security numbers introduces a higher risk to your organization. The Social Security number has been called the "magic key" for identity thieves, by George Washington University law school professor Daniel Solove. Most organizations engaged in volunteer management only need to collect this information for the purpose of performing background checks. This is why VolunteerMatters has chosen to protect the organization/agency and the individual by partnering with services that specialize in the electronic processing of background checks. This essentially outsources the compliance with all federal, state and local regulations related to background checks including the storage of SSNs.

If your organization should still chose to collect and/or store high impact PII in your VolunteerMatters system, be reminded that you the Customer, not Closerware or VolunteerMatters, shall have sole responsibility for the integrity and legality of collecting and storing such data.