PCI DSS, HIPAA and Data Security
FAQs

General Statement

Your donor's payment security is our top priority.

Our technology and processes are reviewed regularly and undergo an annual audit by a PCI- accredited 3rd party to ensure PCI compliance. We are also our own merchant provider, securely processing all your transactions.

We adhere to strict security policies to ensure all interfaces and/or data transfers between systems are encrypted, and we do not scan a client's systems as a part of our validation or store any personal information on our servers.

FAQS

What is HIPAA?

HIPAA aims to protect the confidentiality and security of healthcare information. The Privacy Rule component of the law establishes national standards to protect individuals' medical records and other personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization, including uses for fundraising. Updated HIPAA regulations released in 2013 clarify the rules fundraisers must follow to comply with the statute, and it is important for fundraisers to revisit these modifications to ensure proper adherence.

How does HIPAA relate to Greater Giving?

Since 2002 Greater Giving has provided fundraising software and credit card processing to non-profit organizations and schools. During that time we have worked with hundreds of hospitals and health care providers. We understand that security and confidentiality of patient information is of the utmost importance for organizations that provide medical services to members of the community, just as the security of credit card information of our clients is of utmost importance to Greater Giving.

In order to ensure that security for our clients' data, Greater Giving maintains PCI-DSS certification as a Level 1 Service Provider.

Greater Giving products and services do not interact with patient information and therefore are not required to adhere to HIPAA requirements to protect patient rights and information. Our services provide ways for an organization to interact with donor information that is related to fundraising events and activities. Our products and services are not designed or intended to interact with patient information, therefore we do not sign any documentation concerning HIPAA compliance.

Is Greater Giving PCI DSS compliant?

Greater Giving is a Level 1 vendor, the highest, most secure level of PCI compliance across all our platforms. Our technology and processes are reviewed regularly and undergo an annual audit by a PCI accredited 3rd party to ensure PCI compliance. We are also our own merchant provider, securely processing all your transactions.

Does Greater Giving provide information about tools used?

For security reasons, we do not reveal detailed information about the tools we use, or request approval before using these tools on our own systems.

How can I confirm Greater Giving's current PCI DSS compliance status?

Visa maintains a registry of compliant service providers. You can confirm Greater Giving's presence by going to http://www.visa.com/splisting/index.html. Click on the yellow Search Service Providers button. Type Greater Giving into the Company Name field, and then click on Search, on the lower right hand side of the page.

Is there other security/compliance documentation?

We receive three main documents as a part of the PCI DSS compliance process:
-AOC (Attestation of Compliance)
-ROC (Report on Compliance)
-Vulnerability Scan report

These documents are submitted to PCI as part of the annual compliance audit. For confirmation of our PCI compliance status, please refer to the Visa Global Registry of Service Providers at http://www.visa.com/splisting/index.html.

These specific documents however cannot be shared with a third party, because it would put our security infrastructure at risk. The SSAE 16 (Statement on Standards for Attestation Engagements Number 16) is available by request; which allows Greater Giving to show a third party we do have controls in place to protect data, prevent fraud, etc., without giving specific details which would compromise our security.

Can we access card flow diagrams from Greater Giving?

Greater Giving card flow diagrams can be provided by request for use in understanding the flow of card data in determining PCI compliance, understanding overall risk and for use in documenting compliance under its own internal and external compliance standards.

Is there an automated method in place to synchronize all critical technology clocks and times?

This is covered by PCI DSS Requirement 10.4, which Greater Giving is compliant with.

Are controls in place to prevent changes to audit logs or deletion of audit logs?
Yes, controls are in place to prevent changes or deletions to audit logs.

Are personal identifiers kept on a secure file technology?
Yes, personal identifiers are kept on a secure file technology.

Is source code properly protected from unauthorized access?
Yes, Source code is properly protected from unauthorized access.

How is your data encrypted?
All interfaces and/or data transfers between systems are encrypted. When encryption is used the decryption keys are not tied to user accounts or stored on media. Data is encrypted using industry standard cryptographic protocols.

Passwords are not transmitted or stored nor embedded in clear text including scripts or code and other uses.