



CPAs & ADVISORS

Privacy Checklist

- Does the organization have a privacy policy, which is easily available on the organization's website?
- What information is collected from consumers/members/etc.?
- Is the policy clear about how information that is collected is being used?
- Is personal data shared with any third parties? If yes, do these organizations share the same policies as your organization in regards to privacy and security? Is authorization granted from the individuals prior to sharing this data with other organization?
- Do you know what data the organization has and what it is responsible for? How is it stored? Internal servers, external services, cloud, etc.
- Do employees understand personal data protection policies and procedures?
- Is it known who has access to personal identifiable information (PII)?
- Are data protection policies regularly reviewed and updated?
- Where applicable, are you compliant with regulations? (Ex: HIPAA, PCI, GDPR, CCPA, etc.)
- Do consumers/members/donors/grantors/etc. have the ability to opt-out/opt-in of providing PII
- Does the organization have a data map to show where all PII information is stored?

For more information about privacy risk, visit our website at www.grfcpa.com/accounting-services/advisory-services/cybersecurity-and-it-risk/.