HIPAA and Blackbaud Solutions

The Health Insurance Portability and Accountability Act, as amended ("HIPAA") is a US healthcare law that establishes requirements for the use, disclosure, and protection of individually identifiable health information, known as Protected Health Information ("PHI"). HIPAA applies to "Covered Entities"—healthcare providers, health insurers, and other healthcare companies—with access to patients' PHI, as well as to "Business Associates" that process PHI on their behalf.

The HIPAA Privacy Rule sets forth circumstances when PHI can be disclosed or used and gives patients certain access rights to their PHI. The HIPAA Security Rule requires appropriate administrative, physical, and technical measures to protect the confidentiality, integrity, and security of PHI stored electronically.

Covered Entities using Blackbaud Solutions are responsible for HIPAA compliance with respect to PHI stored in our Solutions to the extent that the Covered Entity affects these factors. For example, a Covered Entity is solely responsible for HIPAA compliance with respect to access to PHI by the Covered Entity or other party through user accounts that are fully under the control of the Covered Entity, for the integrity of PHI uploaded by the Covered Entity, or for security of its own networks.

When Blackbaud is acting as a Business Associate—meaning that PHI is being stored in our Solutions and the parties have entered into a Business Associate Agreement—we comply with the HIPAA Privacy Rule by restricting our use and disclosure of PHI to purposes authorized by you and we comply with the HIPAA Security Rule by providing you with a secure environment for your PHI and adopting strict policies and procedures governing processes that could affect your PHI.

Though third-party audits are not required for HIPAA compliance, we have Blackbaud CRM® audited for HIPAA compliance for service providers by an independent third-party, and it has received an AICPA AT Section 101 standard audit report with no exceptions. This report is available to Blackbaud CRM® customers and prospects upon request. Our remaining Solutions are not yet formally audited by a third-party auditor for HIPAA compliance, but we believe such Solutions are able to comply with HIPAA because of our robust security and privacy program. We use industry-standard security practices, modeled on an ISO 27001 information security governance structure, throughout our solution development lifecycle and when transmitting and storing customer data in Blackbaud Solutions. Our comprehensive security program requires us to take rigorous measures including systematically evaluating and addressing security risks like malicious code, using strict access controls based on the principle of least privilege, using strong encryption, and providing extensive training to our employees.

Blackbaud regularly performs (or has a third party perform) assessments and audits obtaining certain approvals and certifications regarding our compliance with industry-standard data protection protocols. For example, for all our hosted Solutions, a Service Organization Control (SOC) 2 audit gauges the effectiveness of a service provider's system or applications, based on the AICPA Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality and Privacy). A copy of our SOC 2 audit report is available to Blackbaud customers and prospects upon request.

For more information about our security and privacy practices, or to request a HIPAA audit report for Blackbaud CRM® or SOC 2 audit report, please contact your account executive.

September 2017