



Health Privacy and Security Program

Magnus Health Privacy and Security Program

The privacy and security of Personal Health Information (PHI) is a high priority at Magnus Health. That's why we've developed, implemented, and maintain a comprehensive Privacy and Security program. The program contains administrative, technical, and physical safeguards that are appropriate and applicable to our company's size, scope, and type of business, the amount of resources available, the amount of stored data, and the need for security and confidentiality of PHI and PII.

At Magnus Health, we limit access to personal information to only those employees who reasonably need access to that information in order to provide services to you, or to perform their job. All Magnus employees are required to receive an annual internal Privacy and Security training, detailing HIPAA, FERPA, PCI, any applicable updates, expectations, and requirements when handling PHI.

Our philosophy is to take security into account with every feature and service we develop. For example, we encrypt all customer data that travels over the public internet, which includes the transmission of files.¹ We also encrypt each file before long term storage. Finally, all of our security procedures, policies, and processes undergo an annual audit by a third party, up to and including penetration testing.

Annual Privacy and Security Assessments

HIPAA Assessment - Completed annually by Total Medical Compliance, this privacy and security audit reviews both physical and technical security standards, data standards, and risk profiles. All Magnus employees also receive privacy and security training on an annual basis.

PCI Compliance - Annually, Magnus Health completes a questionnaire to maintain our PCI SAQ A Compliance. PCI defines security standards compliance, destruction of data, storage of data, and credit card information standards. Magnus does not store any credit card details, as this is handled via a payment processor that is PCI compliant.

Magnus Health software is the most innovative way to collect, track, and manage student health information.

Health Privacy and Security Program (cont'd.)

TRUSTe Privacy Certification - Conducted annually by TRUSTe, this audit reviews terms and conditions on the Magnus website and confirms their compliance with TRUSTe's nationally-recognized program requirements.

Penetration Testing - Completed annually by a third-party, this test is performed by software intrusion specialists to test the vulnerability of product code, infrastructure, and employees. They make physical and social attacks on Magnus Health systems to find any areas of potential breach.

Student Privacy Pledge - Magnus Health is an annual signatory of the Student Privacy Pledge. By signing this pledge, we have agreed to carry out responsible stewardship and appropriate use of student personal information in accordance with the commitments set by the Student Privacy Pledge, and all laws applicable to us as school service providers.

CONTACT US

For further inquiries regarding the Magnus Health Privacy and Security program, please contact the Privacy Committee at privacy@magnushealth.com. For more information on our [Privacy Policy](#), you may visit the privacy page on the Magnus website.

¹ *Emails sent to and from Magnus applications are not encrypted. Magnus has taken reasonable efforts to exclude PHI and PII from email content. Please consider the nature and content of emails prior to sending communication to parents, students, and the Magnus Health Support Team. Emails containing PHI will not be accepted by Magnus.*

Magnus Health software is the most innovative way to collect, track, and manage student health information.