HIPAA COMPLIANCE STATEMENT

COMPLIANCE

Magellan Health, Inc. (Magellan) is fully compliant with the HIPAA Standards for Privacy, Electronic Transactions and Security. Magellan's Corporate Compliance Department works in conjunction with each of Magellan's business units, departments, and regional offices to monitor on-going compliance efforts and maintain various reporting mechanisms that are required by law or requested by Magellan's health plan customers. Magellan recognizes that it is a key business partner with its customers and will continue to provide all of its various Managed Care and EAP services in accordance with the relevant requirements of all state and federal laws and regulations, including, as applicable, HIPAA.

PRIVACY

Magellan has historically held the privacy of patient information as a key tenet of our operations and processes. Magellan has always implemented policies and procedures for confidentiality that met or exceeded existing state and federal regulations. Our many existing policies detailing compliance with HIPAA and all its implementing regulations (including the HITECH Act and the Omnibus Rule of 2013 as well) and other privacy-related requirements include:

- Authorization to Use and Disclose PHI (Protected Health Information)
- General Rules for Uses & Disclosures of PHI
- Uses & Disclosures of PHI for Treatment, Payment, & Health Care Operations
- Oral & Written Transmission of PHI
- Member Right to Request Privacy Protection of PHI
- Member Right to Request Access to PHI
- Member Right to Request Amendment of PHI
- Member Right to Request an Accounting of Disclosure of PHI
- Verification Policy
- Member Representation
- Notice of Privacy Practices
- Minimum Necessary Uses and Disclosures of PHI
- Uses & Disclosures of PHI Requiring No Permission From the Member

- Uses & Disclosures of PHI for Marketing, Fundraising, and Underwriting
- Uses & Disclosures for Specialized Government Functions
- Uses & Disclosures of PHI Requiring Prior Internal Approval
- Uses & Disclosures of PHI for Judicial & Administrative Proceedings
- Limited Data Set and De-Identification of PHI
- Unauthorized Uses & Disclosures of PHI

For example, these policies touch on some of the following areas:

Confidential Communications

Magellan has developed policies, procedures, and workflows to address confidential communications. We also work with our clients to implement procedures to coordinate member requests for alternative addresses or methods of communicating PHI.

Accounting of Disclosures

Through HIPAA, members have the right to receive an accounting of certain disclosures of their PHI made by covered entities in the six years prior to the date on which the accounting was requested. Magellan has developed and implemented a database to manage the tracking of all disclosures for which members have a right to an accounting. We will also perform routine audits conducted by our Corporate Compliance Department.

Right of Access and Amendment

Members have a right to inspect and copy PHI about themselves, which allows them to understand the nature of their health information and ask that we amend or correct any perceived errors. Members can also request that their access be furnished by sending a copy to another person specifically designated by the member including identifying the designated individual and how/where to send the copy of the PHI. Magellan has procedures in place to protect these member rights.

In sum, Magellan currently complies with all applicable federal and state laws regarding the confidentiality of PHI. Magellan provides HIPAA training to its staff with an emphasis on patient privacy and confidentiality. In cases where the clinical staff believes that HIPAA may be pre-empted by state law or where HIPAA pre-empts state law, they refer their questions to the company's Legal Department. The Legal Department answers the questions based on a pre-emption analysis to ensure we are in compliance with the more stringent of the two laws.

TRANSACTIONS AND CODE SETS

Magellan is in full compliance with the HIPAA Transactions and Code Sets regulation and has taken a leadership position within the industry by working to establish the accepted code sets for managed behavioral health care with the national standard-setting groups.

Magellan is compliant with ANSI X12N, Version 5010 with the Addenda. In meeting the challenge of complying with the Transaction and Code Sets requirements, we have completed the development of a new Electronic Data Interchange (EDI) strategy. We have implemented EDIFEC's software products: XEngine (version 8.4.1.3398), XEServer (version 8.4.0.4017), and Transaction Management (version 8.5.1.7) for message exchange between software applications, computing platforms, and communications protocols. Magellan will use XEngine to validate that the messages are X12-compliant and then parses the X12 into individual elements for mapping information to our host systems for processing. This product suite includes the templates for the HIPAA standard transactions.

SECURITY

Magellan's Office of Information Security (OIS), Personnel Security and Physical Security have the task of ensuring that members' health information is protected as it rests in our systems and when it is exchanged via electronic means. To address this, we have implemented technical, physical, and administrative safeguards to enhance:

- Physical Security
- Personnel Security
- Information Security

Magellan has taken a multi-layered approach to security, providing perimeter protection, segregated operations, business, and administrative architectures, and extra protective measures associated with our World Wide Web presence. Magellan also monitors all of these interfaces to identify inappropriate or unauthorized traffic, e-mail, and attempts to connect to our systems.

Magellan has drafted and ratified security policies and procedures to meet compliance standards as well as solidify best security business practices. Procedures have been implemented to support these policies in a manner which complements and follows each policy to ensure standardization. Policies that have been ratified to date include:

- Information Technology Security
- Information Sensitivity
- Disaster Preparedness
- Remote Network Access
- Internet Usage
- Computer and Network Usage

- Employee E-mail Usage
- Pre-Employment Background Investigation
- Termination of Security Accesses for Employees and Contractors

Firewalls/Intrusion Detection Services (IDS)

Magellan employs the latest technology standards and equipment regarding the protection of the critical internal infrastructure. All firewalls are deployed, monitored, and managed by qualified, dedicated Magellan personnel. All perimeter protection equipment is installed, patched, and maintained in accordance with manufacturer standards and best security practices to ensure best possible protection.

A traditional DMZ (de-militarized zone) structure is in place to support our e-commerce needs and is monitored via a state of the art managed intrusion detection systems provided by an external organization to ensure quality of service. The IDS service is monitored 24 hours a day, seven days a week, 365 days a year by IBM, Inc., which specializes in incident response and intrusion detection capabilities for various corporations world-wide.

Systems Activity Audit/Monitor

All systems activity, including user activity, is monitored in accordance with policy. All deviations from accepted practices outlined in policy will be investigated and risks associated with these events will be mitigated accordingly.

Encryption Capabilities

E-mail

The security of Magellan e-mail communications requires a blending of several (three) technologies to provide a diverse and flexible method of delivery. The method will involve the use of Virtual Private Networks (VPN) or dedicated links, an encrypting e-mail gateway, and a Web-based secure e-mail portal.

Wide Area Network (WAN)

All WAN connections are encrypted to industry standards. All WAN connections are managed by qualified, dedicated Magellan personnel.

World Wide Web (Internet)

All of the Magellan Internet facing Web sites incorporates the usage of Transport Layer Security (TLS) protocol versions 1.1 and 1.2 to protect sensitive information.

Release of Magellan Proprietary Network/System Specific Information

It is Magellan's policy not to disclose specifics regarding the detailed flowcharts and technical specifications of the software, hardware, and networks Magellan uses to construct its technical infrastructure. Specific details may be provided if appropriate non-disclosure agreements are executed between Magellan and the requesting party.

Vulnerability Assessments

Magellan routinely conducts security assessments and vulnerability testing and mitigates any issues or risks found in a timely manner. It is our policy not to disclose specifics regarding details or results of testing due to the proprietary and sensitive nature of the data. Magellan uses industry standard testing tool-sets and engages third-party, independent agencies to verify security infrastructure.

Data Center Facilities

Magellan's systems are housed in a secured data center located in Maryland Heights, Missouri. Access to the Data Center is controlled through a variety of physical security processes. Physical access is controlled by door, time of day, and day of the week, including holidays and weekends. System operators staff the Data Center 24 hours a day, seven days a week, 365 days a year.

Nightly backups are performed to capture changes or updates. Full backups are performed on a regular basis. Back-up tapes are stored at an off-site facility.

The Information Technology system is provided short-term back-up power through Uninterrupted Power Supply (UPS). A back-up diesel generator provides long-term power supply back-up. Tests are performed periodically to provide proficiency and assess effectiveness of these systems.

The Data Center is protected against fire by a fire protection and alarm system. The detection system is connected to a building alarm panel and the local fire department for immediate notification. The Data Center uses a gas fire suppression system, a dry pipe sprinkler system, and was constructed with highly rated fire resistant walls.

Disaster Recovery

Magellan has contracted with SunGard Availability Services to provide a pre-configured warm site and standby hardware located in Philadelphia, Pennsylvania to facilitate the continuation of data processing services performed on the computer systems in the event of a catastrophic disaster. Our approach addresses the following items:

- Potential types of disasters, risks, and probabilities of occurrence that would result in a significant disruption to successful operations
- Contingency plans to ensure continued operations and minimize impact
- A recovery strategy and process that defines roles and responsibilities during the period
- Critical business functions and the maximum tolerable interruption period
- Resources required to implement a successful recovery

ON-GOING COMPLIANCE

Magellan's Corporate Compliance Department is charged with overseeing ongoing compliance with the HIPAA regulations. This department is staffed by attorneys, compliance directors, and research analysts who work together to monitor any new developments and coordinate any necessary implementation of updated compliance requirements. Our HIPAA Training Program consists of initial training for all new hires, annual training refreshers for all employees, in-depth training for targeted areas, and remedial training on an "as-needed" basis. An internal auditing department audits corporate departments and regional offices to ensure appropriate compliance measures and procedures are in place.