UNITEDHEALTH GROUP®

Information Technology

How UnitedHealth Group Protects Customer Data

UnitedHealth Group understands the responsibility it has to protect confidential and proprietary information and to maintain availability and integrity of information systems and assets. This commitment is integral to the relationships we have with all of our customers and vendors alike.

Information Security Program

UnitedHealth Group manages and supports a robust Information Security Program. Its protocols are based on industry practices, all applicable regulatory obligations, and customer considerations. Policies and standards are used to manage the specific requirements and basic premise of general computing, audit, and security controls.

The Information Security Policies and Standards represent the foundation of security applied to and within the UnitedHealth Group proprietary network infrastructure and critical application services. These controls are reviewed on an annual basis.

The requirements of the HIPAA Security Rule are reflected in the Information Security Program.

Monitoring and Security

UnitedHealth Group information technology systems and network activity are monitored for unauthorized actions to ensure information security controls are not tampered with or bypassed.

All UnitedHealth Group network connections, whether outbound or inbound, are filtered through a corporate approved firewall, layers of firewalls and/or isolated from internal network connections. The firewalls are configured to protect against unauthorized intrusions and limit external access to the internal company networks. Industry standard Intrusion Detection Systems are in place to enable the detection and response to information technology system intrusion events.

Data at Rest

UnitedHealth Group currently encrypts data at rest in areas where our information risk management program indicates that additional safeguards are warranted. Encryption considerations are addressed for workstations, backup media and disk storage.

In addition to encryption, additional sophisticated inventory management and on-site media destruction guidance exist for backup media and disk storage devices respectively.

Disaster Recovery

UnitedHealth Group's approach to disaster recovery is based on the two fundamentals: prevention and protection. A focus on balancing the combination of disaster prevention and protection results in reducing both the probability and impact of a disaster. The Enterprise Disaster Recovery Program first eliminates or reduces disaster recovery risk in critical areas, and then plans for the most probable disaster scenarios.

UnitedHealth Group has invested in creating an effective combination of people, process and technology that provides the fundamentals for a proven production method resulting in a stable, scalable environment for our applications to perform at operational excellence. This investment creates the "prevention" which is fundamental to the Enterprise Disaster Recovery Program. Prevention is the proactive remediation of known technology exposures. Prevention includes removing the "accidents just waiting to happen".

Completely avoiding a technology disaster is impossible. However, the Enterprise Disaster Recovery

Program is based on anticipating and planning for the common types of disasters and designing solutions to address them. Disaster Protection addresses recovery from the most probable disaster scenarios and a worst case “smoking hole” scenario.

The UnitedHealth Group Information Technology enterprise disaster recovery strategy involves identifying critical business processes and transitioning these critical applications, data, and supporting infrastructure to an alternate recovery location in a timely manner, thereby reducing the impact of a technology event to our critical business clients.

A variety of recovery strategies are utilized which align to the defined criticality of the application. Business continuity plans are updated quarterly and monitored for compliance by the Enterprise Resiliency & Response office.

Existing Disaster Recovery Plans follow standard lifecycle maintenance and are refreshed at least annually.

HIPAA/HITECH

UnitedHealth Group is in compliance with HIPAA/HITECH requirements. UnitedHealth Group’s security program is designed to satisfy all applicable security requirements and regulations, including the HIPAA Security Rule.

A number of periodic external and internal general computing and security control reviews are performed to provide a continuous, systemic and cohesive assessment of the Company's security controls. Information security controls may also be tested by regulators, such as the Department of Insurance. As a separate internal activity, UnitedHealth Group conducts specific assessments against the HIPAA Security Rule requirements.

Appropriate mitigation/remediation actions are implemented in the event potential control issues are identified, as determined by the UnitedHealth Group Risk Management Process.