ENTERPRISE INFORMATION SECURITY

UnitedHealth Group is committed to strong cybersecurity and data protection practices designed to protect the confidentiality, availability, and integrity of our information systems and assets. Through our Enterprise Information Security Program, we continue to focus on deploying leading security practices to stay apace with evolving cybersecurity threats and risks to customer data.

CYBERSECURITY THREAT LANDSCAPE

Rise in Health Care Cyber Attacks

- External and significant attack attempts against health care companies continue
- Rise in malware and ransomware
- External attack attempts and scans of our most visible branded applications
- Sophisticated spear phishing targets individual employees by function, class

Top Two Threats by Volume and Impact: Social Engineering & Malware for Profit

- **Ransomware is a rapidly emerging cyber threat in the healthcare industry**.
- Ransomware is disruptive to operations, will impair systems, make data unusable (possibly beyond repair), and demand a ransom before data/services are released to the victim.
- **Increased Global Cybercrime:** Modern tools and pervasive "Crime-as-a-Service" infrastructure enable attackers to operate on a global scale at zero day speed.

- **Ever Vigilant:** We have enterprise visibility into log events and network traffic. We utilize best-in-class tools and capabilities to detect and block malicious activity.
- **Continuous Awareness:** Ongoing operational tests for cyber resilience and social engineering across our operations, training, phishing campaigns and measuring the effectiveness in response, while maintaining critical business functions.
- **Global Security Intelligence:** UnitedHealth Group's Investigative Services deploy world-class threat hunting, digital forensics services and data scientists to sustain and leverage one of the largest security event data lakes in industry.

WHY US?

WHY HEALTH CARE?

- Health care information provides rich data sources of intellectual property and for identity theft scenarios
- Rapid growth of technology and the transformation of healthcare innovation disrupts traditional systems

Cyber Threats Facing Health Care

- Health care continues to be a target of sophisticated cybersecurity attacks with ransomware most prevalent
- Breaches of major services such as Yahoo, LinkedIn, Dropbox and Equifax extend the risk of stolen credentials and identity information being used in other attacks
- Increased regulatory activity specific to cybersecurity has been seen in the United States and the European Union
- Political conflicts between countries will facilitate increasing cyber espionage, cyber attacks and hacker activism

CYBER DEFENSE SYSTEMS

Over
500
dedicated resources

Security Operations Center evaluates more than a
trillion
events annually

Over
10 Petabytes
of big data used to advance security analytics

Security Operations Center with integrated intelligence from Government, Industry (Domestic and International)

Vulnerability Management responding to vulnerabilities including “Red and Blue Team” exercises that test the effectiveness of our information security program and defense capabilities through simulated attacks

Security Intelligence Relationships with government agencies and external cyber intelligence communities (FS-ISAC and HITRUST CTX)

Security Big Data enhanced data collection and event correlation capabilities analytics and insight

24x7 Command Center, Cyber Forensic and Security Incident Response capabilities, frequently tested and hardened

Risk Profile

- >200,000+ Workstation computers
- 80+ Billion transactions annually
- 1 Billion annual portal transactions
- 902 Million claims per year
- 6.4 Million annual batch jobs processed
- 78 Terabyte secure external data transfer
- 90% transactions received via electronic data interchange (EDI)
- Over 24 million personal health records
- Virtual Contact Center supports 192 million calls
- 19 Million files securely transferred annually
- 60,000+ servers

Information Security

- Integrated cyber defense capabilities
- Evolving security protections in response to new threats
- Cross industry collaboration
- Security agility for commercial operations

Protect the Company
Security Capabilities

Meet Obligations
Compliance Oversight

UNITEDHEALTH GROUP KEY SECURITY OBJECTIVES

Industry Leading Security Framework to Protect Data, Leverage Technology and Deliver Best in Class Security Operations and Services

- Focus on deploying leading security technology for perimeter defense of network computing assets
- Implemented workstation technology to reduce device theft, compromise and credential loss
- Benchmark our programs with the defense industry and HITRUST
- Enhanced control measures for privileged accounts through password vaulting and monitoring
- Deployment of big data analytics for security events
- Deployment of multi-factor access technology including Smart Cards and Tokens
- Enhanced vendor contract control requirements including certification (i.e. HITRUST) for high-risk vendors and suppliers

HOW WE PROTECT OUR DATA

UNITEDHEALTH GROUP RECEIVES

11 MILLION

EMAILS A DAY FROM EXTERNAL SOURCES

WE MONITOR OUR SYSTEM

24X7X365

IN REAL TIME

90%

OF THE EMAILS ARE BLOCKED DUE TO VARIOUS SECURITY REASONS

OUR FIREWALL DEFENSES OBSERVE OVER

800 MILLION

EVENTS A DAY

Continued Response and Focus

- Ransomware response program continually updated with resilience planning and employee awareness
- Denial of Service defenses with embedded multi-carrier strategy
- Ongoing access protocol assessments to include multifactor and risk based authentication protocols
- Embedded cyber intelligence services to facilitate proactive threat response measures across critical services

VENDOR RISK MANAGEMENT

UnitedHealthcare Business Expertise

The moment risk assessments are performed by Enterprise Information Security (EIS), the UnitedHealthcare Vendor Management Office (VMO) partners with EIS and the vendors to review the findings, agree on mitigating activities, and sets forth 'trust but verify' processes until the risks are effectively cleared.

In 2016, thousands of risk assessment findings were identified and closed across hundreds of our highest tiered vendors.

In addition to aggressive risk remediation, the VMO looks across the entire UnitedHealthcare business control environment to stay apace with evolving cyber security threats:

- **VMO approval and appropriate EIS risk assessment** are required for all new vendors prior to the sharing of protected health information (PHI).
- **Smart and targeted vendor consolidation** continues to drive the most effective risk mitigation results. In 2016, UnitedHealthcare vendors were reduced by nearly 20 percent.
- **Vendor data sharing methods** are thoroughly examined to minimize the volume of sensitive data sent outside our firewalls.

For additional information about our Enterprise Information Security, contact your UnitedHealthcare representative.

UNITEDHEALTH GROUP®

UnitedHealth Group
9900 Bren Road East, Minnetonka, MN 55343

September 2017