Anthem Information Security Workforce Information Security Program (WISP) Overview

Abstract:	This document provides an overview of Anthem's Information Security Program and its key elements.
Owner:	Chief Information Security Officer
Classification:	Limited Distribution
Distribution:	Approved for internal dissemination to workforce members, subsidiaries and affiliates. Approved for external release to business partners.
Version:	1.6
Initial Issue Date:	December 3, 2014
Last Revised:	May 22, 2019
Last Annual Review:	January 28, 2019

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

Table of Contents

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

1 - Introduction

1.1 Anthem's Commitment

One of Anthem's Values and Behaviors is being trustworthy, and this means:

- We do the right thing.
- We are transparent in words and deeds.
- We keep our commitments.

Anthem is committed to protecting customer data and demonstrating how we are a trustworthy business partner. Key to Anthem fulfilling this commitment is ensuring that as we serve our customers, we do it in a manner that maintains customer trust. Information Security is dedicated to the task of maintaining that trust by:

- Partnering with business areas and IT to protect our information assets from compromise.
- Enabling business areas and IT to focus on providing the services our customers want.
- Providing a clear and accessible structure through which organizational information security can be implemented and achieved.

1.2 The Need for Information Security

Anthem is highly dependent on people, processes and technology for its success. The integration of people, processes, and technology is a requirement for business survival and a necessity for Anthem to remain both competitive and profitable. Enhancements in automated systems and technology add value, increase productivity and improve capability; but they also create a higher level of business dependency and thus increase risk. These risks can be broadly classified as:

- Internal manipulation of systems and information for fraudulent purposes.
- Unauthorized internal or external access to systems and information for the purpose of fraud, identity theft, access to competitive business intelligence or Covered Information or other Confidential Information, sabotage and other criminal acts.
- Intentional and unintentional damage to systems or data by unauthorized users and by associates or as the result of weak or non-existent security controls.
- Business interruption caused by natural or manmade disasters, computer viruses, equipment failure or security breaches, which result in the loss of productivity, business and revenue.

Anthem realizes that it must rely on both established and emerging technology in order to provide superior value to its customers. Anthem also realizes that (i) this reliance must be balanced against an acceptable level of risk, (ii) these technology risks need to be properly evaluated, monitored and controlled, and (iii) necessary security controls, mechanisms and programs need to be in place to protect corporate information assets.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

1.3 The Role of Information Security

The thousands of workforce members at Anthem are our strongest advocates for the security of Anthem systems and the personal information of our customers. It is with people that the success of the Program will be determined. However, the best intentions of workforce members alone will not ensure adequate security. Information Security must develop and deploy a program that enables workforce members to meet security objectives while excelling at their jobs.

Just as technology enables business to succeed, Anthem can strategically deploy Information Security tools and systems that enable our people and processes to function at increasing levels of proficiency. However security cannot be gained by simply deploying a tool or product. Effective people and processes designed to ensure technology adds value to the organization must be in place.

1.4 Program Overview

The Anthem Chief Information Security Officer (CISO) owns the Anthem Workforce Information Security Program (WISP) and is responsible for managing the Program and developing, implementing and enforcing the Program's Policy Statements. The CISO will provide periodic reports regarding the status of the Program and the overall state of corporate security to the Chief Information Officer (CIO), Senior Leadership Team (SLT), Executive Leadership Team (ELT), Chief Executive Officer (CEO), and Anthem Board of Directors as may be necessary or appropriate.

The overall objective of the WISP is to establish effective corporate-wide policies, standards, procedures, guidelines, and strategies that address the security of Anthem computer resources, infrastructure, data and information assets regardless of the party responsible for use or management, the physical location or the medium in which such information assets reside (e.g., electronic, digital, paper, etc.). The WISP is based in part on Anthem's risk assessment processes and reflects the application of relevant IT controls including:

- Regulatory requirements, such as HIPAA, HITECH, and PCI
- Industry frameworks and standards, such as HITRUST
- Anthem Information Security policies and standards

At a minimum the WISP consists of the following:

- The basic protection requirements for all stored information and data, and the requirements that must be followed by anyone who uses a computer system, software program or other information asset owned by Anthem.
- The internal publication of Foundation Documents consisting of policies, programs, standards, procedures and guidelines that address the technical implementation, control, management, auditing and administration of computer security and information asset protection.
- The development of baseline requirements for the physical protection of Anthem's technology infrastructure.

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

- The implementation of an information security awareness program to assist in the education of all corporate associates and help reduce levels of risk associated with electronic data processing and computer system usage.
- The implementation of an information security administration function responsible for coordinating and administering requests for user access to Anthem computer systems and data resources, removing access to these resources when no longer required and performing routine audits to validate that security protection mechanisms are functioning properly.
- The implementation of a security risk management function to assess, manage and communicate risks to Anthem assets and the actions to be taken to mitigate these risks.
- The establishment of mechanisms to monitor, analyze and report on the effectiveness of the Anthem Workforce Information Security Program.
- The appropriate controls that allow us to adhere to applicable federal and state regulations, international law, legal requirements and best practices.
- The maintenance of liaison relationships with internal and external organizations and departments.

At a minimum, the WISP is reviewed on an annual basis, or as new vulnerabilities and threats become known, and new business, technology and regulatory requirements are identified. The CISO and all Information Security staff are committed to continuous review, improvement and maturation of the WISP.

1.5 Program Goals and Objectives

The objective of this document is to define the guiding principles and framework used to maintain the Confidentiality, Integrity and Availability of Anthem information resources. The goal of the Program is to properly secure all corporate information assets while still facilitating the access needed for the business to run smoothly and efficiently. This goal will be accomplished by implementing mechanisms and controls which require that:

- No unauthorized changes to systems or data occur that compromise system integrity or data accuracy.
- Computing systems and information resources are available or have appropriate contingencies in place that provide timely and reliable service.
- Implemented controls are justified and efficient so as not to adversely impact operations and business usability.
- The privacy and protection of Covered Information is maintained.
- Information security controls are implemented to satisfy the compliance requirements of applicable laws, regulations and standards.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

2 - Information Security Program Safeguards

2.1 Access Control

Access Control governs establishing, activating, modifying, disabling, expiring and removing of accounts and access permissions. This includes processes and standards for managing user access based on need to know (least privilege), separation of duties, and scope of user responsibilities. The Access Control safeguard addresses role-based access (including formal audits, reviews, and approvals), access account administrator responsibilities, the process and standards for user validation, and related access control mechanisms, including mobile and wireless access. The WISP also addresses remote access methods and requirements.

2.2 Audit and Accountability

Audit and Accountability requires that a risk-based process be established, implemented, and maintained for identifying and auditing security events, the frequency of audits, the actions to be taken for audited events, and reporting mechanisms. This includes tools for audit information collection, the logging of security events, and the review and retention of logging performed on Privileged Accounts usage and other higher-risk activities. In addition, data balancing and validation controls are addressed in this section.

2.3 Awareness Training

The WISP sets requirements for security awareness training that communicates workforce member information security responsibilities. In addition to updated awareness training content, periodic reminders on security risks and best practices are also communicated via intranet news articles and email. This section also provides training frequency requirements, targeted audiences and relevant content for each audience, and maintaining records of training provided to workforce members.

2.4 Cloud Computing Security

This section addresses the use of cloud computing-based services and platforms and the requirements needed to support various models. The following cloud computing security terms are covered: cloud computing, multi-tenancy, public clouds, private clouds, and hybrid clouds. (See Section 3, Definitions, Acronyms, & Abbreviations, for their definitions.)

Anthem enables information assurance by classifying data and creating meaningful boundaries to provide separation between information communication media and between data types. The basic building blocks of separation are physical and logical controls. Anthem employs segregation and isolation of data to assure data is accessed and used appropriately. This includes logical controls, virtual machine zoning, virtualization security, and segregation for multi-tenancy environments. Anthem requires FIPS 140-2 approved encryption methods in a multi-tenant environment for hosting Covered Information in transit, storage, and at rest for cloud-based computing. Appropriate key management is required.

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

Cloud Service Providers are required to provide a mechanism to meet data legal hold and metadata requirements, and they must complete an annual independent audit of their environment. Logging and audit of identity, credentialing, authentication, authorization, and access control events are required to be in compliance with Anthem access review standards and the provisioning of account management capabilities for Anthem. Identity management for cloud computing-based services is performed via authentication and authorization against Anthem US Domain users.

Anthem requires incident response roles and responsibilities to be established for the cloud service provider and Anthem. In addition, reporting requirements for vulnerability scans, intrusion detection, and identity management will be established and implemented.

2.5 Compliance

Compliance requires that security controls, review processes and protection strategies are in place to safeguard assets and Confidential Information in a manner consistent with applicable laws, regulations and standards.

Appropriate logical and physical security controls must be implemented to maintain compliance with applicable laws, regulations and standards. At Anthem, Information Security is responsible to establish the security requirements that will be followed to implement compliance. For differing lines of business, these can include but are not limited to:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Sarbanes-Oxley Act of 2002
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing regulations (45 C.F.R. Parts 160-64)
- Individual state privacy laws
- Individual state security laws
- Any applicable implementing regulations issued by the Insurance Commissioner or other regulatory authority having jurisdiction and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”)
- Any regulations adopted or to be adopted pursuant to the HITECH Act that relate to the obligations of business associates
- Gramm-Leach-Bliley Act (GLBA)
- Fair and Accurate Credit Transaction Act (FACTA)
- Federal Information Security Management Act (FISMA)

This section includes providing mechanisms for monitoring compliance.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

2.6 Confidential Financial Information Security Requirements

This section establishes requirements for the protection of Confidential Financial Information. Confidential Financial Information includes Protected Financial Information as defined in Anthem's Corporate Privacy Policy and Procedure Glossary, as well as any financial information belonging to an individual or organization that includes:

- Cardholder data (Credit Card information)
- Automated Clearing House (ACH) information
- Electronic Funds Transfer (EFT) Information
- Account numbers
- Routing codes

Confidential Financial Information must be protected through masking or redacting the account information, and/or through the periodic validation of access account permissions.

2.7 Configuration Management

Configuration Management requires that modifications to hardware, firmware, software, and documentation be controlled on Information Systems to protect against improper modifications prior to, during, and after system implementation in order to maintain Confidentiality, Integrity, or Availability of systems. This is supported by the development of version controlled baseline technical configuration standards as well as the incorporation of compliance oversight and reporting. Anthem has change management policies and processes in place to help ensure changes or updates are not only authorized, but changes are also performed by authorized persons. This includes, but is not limited to the consideration of system capacity and resource planning, security controls for system and application development, testing, validating, and documenting of changes prior to implementations. Anthem maintains an inventory of database systems and maintains a patch management process to address system performance and vulnerability management. Anthem also requires monitoring of database systems in addition to defined auditing and logging requirements. Anthem does not allow the use of non-production systems in a production environment. In addition, Anthem requires implementation of a network segmentation framework to control network access by using purpose-based Security Zones (e.g. development, staging, production) to segment servers.

2.8 Contingency Planning

Contingency Planning ensures that adequate business continuity and disaster recovery plans are developed, documented, and tested to provide for the resumption and continued functioning of vital and critical services and processes of the organization, while protecting electronic health information during emergencies or disasters. Contingency planning includes off-site storage and agreements, alternate processing sites, emergency access to physical and logical assets, and backups of critical information and systems for recovery. This section addresses the periodic review and approval of disaster recovery plans used to prioritize and recover information systems to a known state after a disruption, compromise, or failure.

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

2.9 Email and Messaging System Security Requirements

This section establishes requirements for the use of corporate Email and Messaging Systems, and the use of personal Email and Messaging Systems on the corporate network. Email and Messaging Systems refers collectively to: Email systems, instant messaging and chat systems, Text messaging systems (such as SMS, MMS, TMS, BBM, iMessage, etc.), Video Conferencing systems, Teleconferencing systems (including telephone-based systems such as InterCall Reservationless-Plus and Voice-Over-IP (VoIP) systems such as Skype or Google Voice), social media systems (such as Facebook, Twitter, LinkedIn, Yammer, Blogger, YouTube, Flickr, Wikipedia, etc.) or the corporate accounts and pages established on those systems.

Anthem does not allow the use of non-corporate Email and Messaging Systems when conducting company business, and there is no expectation of privacy for anything stored, sent, or received on corporate Email and Messaging Systems. The forwarding of business-related messages and documents from corporate Email and Messaging Systems to non-corporate systems for purposes other than conducting company business is restricted.

External transmission of Confidential Information via instant messaging and chat systems is prohibited. The use of SMS text messaging that infers or uses Protected Health Information for member outreach is permitted if specific Information Security and Privacy Office requirements are met. Otherwise, transmission of Confidential Information via text messaging or social media systems is prohibited unless required by law.

Access to the non-corporate Email and Messaging Systems is blocked on corporate desktops and laptops from Anthem's facilities, and on laptops and desktops connecting remotely via VPN. In addition, Anthem requires the use of Malware scanning of all attachments received through Email and Messaging Systems as well as additional encryption requirements for securely communicating Confidential Information with external parties. All messages sent to external email systems will have a confidentiality notice appended to them, and all messages sent or received through Email and Messaging systems will be retained in accordance to the Records Management Program.

2.10 Identification and Authentication

Identification and Authentication ensures unique verification of the identity of a user, process, or device through the use of specific credentials (such as the use of passwords and/or token cards) as a prerequisite for granting access to resources (e.g. applications, databases, servers, network, and cryptographic modules) in an information system. This section addresses creating and maintaining secure passwords by defining storage, construction, and complexity requirements. This includes enforcing a limit on the number of invalid user attempts made before lock out, monitoring all access attempts, and reporting violations.

Multifactor authentication is required for remote access, wireless network access, and when using administrative accounts.

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

2.11 Information Security Incident Response Plan Program

Information Security Incident Response Plan Program is designed to manage, communicate, conduct and coordinate all incident response and investigations regarding information technology or related to the use or misuse of corporate computer systems, applications, data, or resources for Anthem and its subsidiaries. This program encompasses three core phases: investigations of incidents, incident response planning, and incident notification and reporting.

2.12 Maintenance

The program ensures that security is enforced throughout the process of performing secure local or remote maintenance on information systems and facilities. This includes maintaining records documenting hardware movements, repairs, and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks), including: identification of the individuals who requested, approved, and performed the maintenance; the date and time of the maintenance; and the description, purpose, scope, and location of the maintenance. The records for maintenance performed on information systems and facilities will be controlled. Security controls will be maintained and documented throughout the process of performing maintenance on information systems and facilities. Continued availability and integrity will be maintained.

2.13 Management of File Shares and Business Collaboration Platforms

This section establishes requirements for the protection of information stored on File Shares and Business Collaboration Platforms (FS/BCPs) internal to Anthem use only. It should be noted that storage on media, mobile computing devices, and corporate application databases are not in scope for this section. Anthem defines FS/BCPs as follows:

- **File Shares** refer to network server-based computer file storage locations that can be used by workforce members to store and share information. Access can be given to one or many users, and administration is performed centrally by access administrators.
- **Business Collaboration Platforms** refer to technology platforms designed to provide workforce members with collaboration spaces and document management capabilities through an application interface. Access is designed to be provisioned to many users. Administration is typically decentralized to the owners of collaboration spaces. Decentralization of end-user administration for Business Collaboration Platforms is a key benefit offering flexibility and speed in the management process. Examples of Business Collaboration Platforms include Microsoft SharePoint and similar platforms.

Anthem requires owner identification for all FS/BCPs, and that required security standards are applied at the time of provisioning. Classification and labeling of FS/BCPs is required to protect against unauthorized disclosure of Confidential Information. Anthem requires the owners of FS/BCPs to determine if Confidential Information will be permitted on the FS/BCPs as well as notifying users of any Confidential Information storage restrictions.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

2.14 Media Protection

Media Protection ensures appropriate security processes and procedures are in place for the handling, transportation, and use of physical media. Anthem defines media as the following:

- **Removable Media** refers to media that are being used for the physical transportation or offline storage of information. Examples include:
  - USB flash drives, compact flash cards, eSATA removable drives, Firewire connected devices, memory cards, Thunderbolt storage devices (MAC OSX only), and Media Transfer Protocol (MTP) devices
- **Internal Hard Drives** refer to hard drives within Information Systems used for the storage of information. Typically these include hard drives within workstations, laptops, servers, RAID assemblies, copy machines, network appliances, multi-function devices, or other devices.
- **Tapes** refer to magnetic tape media used for the storage of digital information. Tapes are used most frequently for the long term storage of data.
- **Non-digital Media** refers to media used to store non-digital information. Examples include hardcopy, paper, microfilm, and microfiche.

Anthem requires the safeguarding and secure storage of information used in the workspace and data centers as well as physical and technical security measures to be used for protecting Confidential or Limited Distribution Information, including prohibiting placing data on Removable Media unless management approval is granted. As an additional technical control, all workstations and removable media are required to be encrypted to support administrative policies for Media Protection. In addition, Anthem requires the use of approved techniques and authorized workforce members to handle and destroy Anthem information on these media types, which may include shredding, pulverizing, incineration, and degaussing (wiping) methods. Requirements for sending, transmitting, transportation, mailing, and management of removable media containing Confidential or Limited Distribution Information as well as the approved encryption methods are included in this section.

2.15 Mobile Computing Devices

Mobile Computing Devices requires that effective program management controls be in place to ensure the risks associated with Mobile Computing Devices (or "Mobile Devices") are adequately identified and mitigated, and to educate users of these devices on the usage risks and countermeasures through awareness training. Mobile Computing Devices include Laptop Computers, Mobile Communications or Convergence Devices, and Mobile Medical Devices. Anthem defines Mobile Devices as follows:

- **Laptop Computers** are Mobile Computing Devices that utilize the primary components of a traditional desktop computer to enable the user to access and/or store company data, and that include a full desktop operating system such as Microsoft Windows, Mac OS X, or Red-hat Linux.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

- **Mobile Communications or Convergence Devices** are Mobile Computing Devices that enable the user to access and/or store company data, but do not run a full desktop operating system and allow diminished administrative control of the device and operating system to IT staff. Examples of such devices include media players, cellular telephones, digital cameras, audio recording devices, e-Book Readers, tablet computers, iPhones, iPads, Android devices, Blackberry devices, webOS devices, and Windows Phone 7 devices.
- **Mobile Medical Devices** are Mobile Computing Devices used for medical purposes, such as instruments, apparatus, appliances, or health care products (excluding drugs) that contains configurable application and/or embedded computer operating systems that are used for a patient or client for the purpose of:
    - Diagnosis, prevention, monitoring, treatment, or alleviation of disease
    - Diagnosis, monitoring, treatment, or alleviation of or compensation for an injury or handicap
    - Investigation, replacement, or modification of the anatomy or of a physiological process

Anthem uses and requires an Internet-facing authentication portal for access to the internal Anthem Network. Anthem does not allow the registration and connection of non-Anthem Mobile Computing Devices to join the Anthem Active Directory domain. In addition, Mobile Computing Device data is required to meet legal hold requirements when applicable, including returned devices no longer in use. Mobile Communications or Convergence Devices are required to be encrypted, require re-authentication after a specified period of inactivity, and will be automatically wiped after pre-determined invalid password attempts are made.

2.16 PCI-DSS Compliance

As an organization that maintains, processes, or otherwise accesses Cardholder Data, Anthem is responsible to secure that information through the application of a comprehensive Information Security Program, including technical, physical, and administrative controls. To ensure consistent levels of security are maintained across all organizations with access to Cardholder Data, the Payment Card Industry (PCI) Security Standards Council (SSC) has created the Payment Card Industry Data Security Standard (PCI-DSS). Failure to comply with the PCI-DSS may result in financial penalties, security breaches, the loss of member confidence, or the loss of privileges to accept card payments from our members. Anthem complies with the PCI-DSS requirements.

2.17 Personnel Security

Personnel Security ensures appropriate security processes are in place for the selection, employment, and termination of workforce members. This includes the screening of potential workforce members and sanctions for failure to comply with established Information Security policies.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

2.18 Physical and Environmental Protection

Physical and Environmental Protection policies are designed to ensure appropriate protection measures have been implemented to safeguard physical assets including paper records and files, other print media, computer rooms, and the data therein. Computer rooms include data centers, network rooms, server storage areas, data processing facilities, tape and disk storage rooms, telephone switch and PBX rooms, and communication and wiring closets. This section addresses physical security requirements for each of these types of locations and the assets and infrastructure stored within them. Access control requirements and rights are defined for each type of physical location as well as monitoring and reviews where required.

Anthem requires physical access devices to be securely issued, stored, and accessed, and to be changed when they are lost or compromised. Confidential Information on printed materials on or around copiers, printers, or fax machines must be removed or securely stored. Fax machines for after-hour incoming faxes are required to be locked.

Environmental protection controls designed to protect Anthem physical locations and information assets include but are not limited to: emergency power shutoff capabilities, uninterruptible power supplies, emergency lighting, fire suppression systems, fire and water master shutoff mechanisms, physical and environmental hazard and security controls, and dedicated and isolated computing environments for sensitive systems. Anthem requires environmental controls for data centers to be defined, monitored, and maintained.

2.19 Privileged Access Management

This section requires that the allocation and use of Privileged Accounts be restricted, controlled, tracked, and monitored, especially over privileged access rights that allow users to override system controls. A Privileged Account is an account that is correlated to an end-user and is authorized to perform critical system privileged relevant functions that ordinary users are not authorized to perform. These accounts have significant authority within Anthem's information systems, including the capability to override system, security, and audit controls, and the ability to perform server administration, security administration, database administration, system control, or technology management type functions, and includes authorization to activate and/or use Firecall Accounts.

Anthem applies the least privilege access rule in accordance with assigned administrative roles and their levels of responsibilities. Privileged account usage may only be used for actions requiring privileged access rights, must be authorized, and assignment is role-based where applicable using the Privileged Account registration and de-registration process. Any usage of non-role based Privileged Accounts require approval. Anthem requires that the built-in administrative accounts shipped with operating systems, databases, network, and storage devices shall either be disabled or the credential vaulted and regularly rotated, and that default passwords be changed. Unique user IDs are assigned to Privileged Account owners for identification and auditability and will be different than their normal user ID for system access. Password for Privileged Accounts must be changed at least once every 60 days, and Service Accounts at least once every 180 days.

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

Authorizations for special privileged access rights will be reviewed during quarterly System Access Validations (SAV). Privileged operations will be logged and monitored, and auditing and monitoring of Privileged Accounts for non-Privileged Account usage will be performed. Anthem requires protection of audit records for any Privileged Accounts and functions. Privileged Accounts must be vaulted to enable checkout when needed to perform privileged functions.

2.20 Production and Test Data Security

This section addresses the use of data for the purpose of testing application or system functionality.

- Production data is defined as data that contains Confidential Information, or Covered Information for which Data Privatization or de-identification has not been performed.
    - Data Privatization is defined in the System Development Life Cycle (SDLC) as “the masking of sensitive information (PII, PHI, HIPAA, etc.) in a repeatable consistent fashion that still meets all test case requirements.”
- Test Data is defined as data that has been created independent of Confidential Information and contains no Confidential Information (aka dummy data), or Covered Information for which Data Privatization or de-identification has been performed.

Anthem requires data privatization or de-identification of production data for testing, training, and other non-production purposes. De-identification of data will adhere to company privacy procedures. Production data utilized in non-production environments shall be protected with equivalent controls to the production environment. Production data used for non-production purposes will be retained or destroyed in a timely manner.

2.21 Program Management

Program Management requires effective program management controls to be in place and that continual maintenance and administration of these controls exist at a satisfactory level. This includes processes for the plans of action and milestones used for the security program and measures of performance that will be monitored and reported on. Anthem requires risks to organizational operations, assets, and individuals to be managed to management's stated level of acceptable risk and Information Security to be included in the organizational risk management process.

2.22 Risk Assessment

Risk Assessment governs the identification of risks to operations (including mission, functions, image, or reputation), assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls required that would mitigate this impact to a level of risk that is acceptable to management. This section includes requirements for the development and implementation of security risk assessment program, vulnerability management program (including the use of external information sources to improve the Information Security Program), system certification process, and reporting of risk assessment

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

programs for the Chief Information Security Officer (CISO). In addition, requirements include performing periodic technical and non-technical evaluations affecting the security of assets, and conducting perimeter penetration tests to assess the effectiveness of the security program. These programs include policies for the remediation of identified vulnerabilities after risk assignments have been made.

2.23 System and Communications Protection

System and Communication Protection addresses the internal and external transmission of information so that adequate levels of protection exist to safeguard the transmission of information, the integrity of data, and to prevent unauthorized disclosure of Covered Information or other Confidential Information. This section also incorporates requirements to technically control and physically separate and monitor public access to internal network systems and key internal points. In addition, Anthem does not allow storing or hosting Confidential and Covered Information within internet facing or unprotected environments.

2.24 System and Information Integrity

System and Information Integrity requires that the integrity of systems and data be maintained throughout the System Development Life Cycle (SDLC) and operation of systems. Anthem requires incorporation of Information Security considerations and controls into the SDLC, secure coding practices, and the management and retention of output from information systems. This section includes requirements for anti-virus software, malicious code protection, full-disk encryption of workstations, and the monitoring of security relevant events and system attacks as well as the use of security alerts, advisories, and directives from designated external organizations.

2.25 System and Services Acquisition

System and Services Acquisition requires that appropriate security processes are in place to select, implement, evaluate, assess, and utilize products and services from external parties. In addition, Anthem provides requirements for Enterprise Standards Governance technology review team, approvals, and oversight as well as a formal request and approval process to install software on company information system assets.

2.26 Encryption

Encryption addresses the use of Approved Cryptographic Controls and secure transport mechanisms and protocols to protect the integrity and confidentiality of information stored or transmitted over external networks. Anthem has established multiple control requirements for protecting Confidential Information for data in use and at rest. Anthem has also established requirements for a key management program used to support the use of approved cryptographic techniques as well as to protect against modification, loss, destruction, and unauthorized key disclosure.

In addition, Anthem requires full disk encryption for laptops and desktops using Approved Cryptographic Controls as well as any Mobile Computing Devices that store Confidential or Limited Distribution information. Video Conferencing Systems and VoIP Teleconference Systems used for communication across external

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

networks require the use of Approved Cryptographic Controls. The integrity and confidentiality of Confidential Information transmitted over external networks is protected through the use of Approved Cryptographic Controls.

2.27 Vendor Security

This section addresses the requirements when Anthem engages third parties to provide certain services that include access to Confidential Information. This information includes but is not limited to Covered Information (including PHI and PII). Anthem requires agreements with vendors who access, process, communicate, or manage Anthem's Confidential Information or information assets to include Anthem's relevant information security control requirements. A comprehensive assessment process is in place to monitor compliance of key Business Associates with the WISP, Privacy policies, and other governing documents on an ongoing basis. Further, Anthem develops policies for managing the security of external network connections between Anthem and vendors. Anthem does not permit the hosting or storing of Anthem Confidential Information offshore and requires vendors accessing Anthem Confidential Information from offshore locations to comply with specific requirements including technical controls to prevent the Confidential Information from being moved to offshore locations and physical controls for offshore facilities. Remote access by vendors and business partners to Anthem networks requires multifactor authentication.

2.28 Endpoint Security

This section addresses Endpoint Security requirements necessary to protect the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices. Endpoint Security requirements include but are not limited to encryption, antivirus, and firewall solutions as well as host intrusion prevention systems. In addition, Anthem requires remote management of mobile devices as well as prohibiting administration credentials being used for non-administrative functions.

2.29 Information Classification

Information Classification is the allocation of information assets into one of a series of categories and the application of specific controls based on those categories. The classification assigned to an information asset is based on the sensitivity, criticality, and value of the information and determines the appropriate level of protection that will be applied. Anthem classifies all information assets, whether generated internally or externally, under one of the following categories: Confidential, Limited Distribution, and Public. The default classification for information is Confidential.

It is the responsibility of the Business System Owner, or the originator or creator of an information asset, to properly classify and label the asset so that it is afforded sufficient protection when in storage (both physically and logically) and to help protect it from unauthorized access or disclosure.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

3 - Definitions, Acronyms & Abbreviations

3.1 Definitions

Approved Cryptographic Controls: Cryptographic Controls (includes encryption algorithms, encryption tools, encrypted protocols, and encryption management processes) that adhere to the requirements of Federal Information Processing Standards Publication 140-2 Security Requirements for Cryptographic Modules, and are established and approved by the CISO.

availability: The property that data or information is accessible and useable upon demand by an authorized person.

cardholder: Non-consumer or consumer to whom a payment card is issued to or any individual authorized to use the payment card.

Cardholder Data: At a minimum, cardholder data contains the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: Cardholder name, Expiration date, Service code. Additional data elements that may be transmitted or processed as part of a payment transaction include security-related information (card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.

cloud computing: Cloud computing, as defined by the National Institute of Standards and Technology (NIST), is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

computer network: A computer network is a group of two or more computer systems linked together. Examples include local-area networks (LANs) and wide-area networks (WANs).

computer rooms: Includes data centers, network rooms, server storage areas, data processing facilities, tape and disk storage rooms, telephone switch and PBX rooms, and communication and wiring closets.

Confidential (data classification): Encompasses all information that must be disclosed only to those individuals with a business need to know and the legal right to access it. Unauthorized disclosure could have a serious financial, legal or operational impact on the organization. Confidential information includes all Covered information and ePHI.

Confidential Financial Information: Includes Protected Financial Information as defined in the Corporate Privacy Policy and Procedure Glossary as well as any financial information that includes: Cardholder data (Credit Card information), Automated Clearing House (ACH) information, Electronic Funds Transfer (EFT) Information, Account numbers, Routing codes

confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

configuration management: The documented management of Information System settings, and changes to the IT infrastructure throughout the life cycle of an information system in order to minimize the impact to Confidentiality, Integrity, or Availability. Other terms for Configuration Management include change control and change management.

Convergence Devices: Any portable device that enables the user to connect to or transfer Anthem data to a portable telecommunications device. Examples include, but are not limited to, iPhones, iPads, Droids, Blackberrys, and Windows Mobile devices.

Covered Information: As defined in the Privacy Policy's Purpose and General Rules, Covered Information is:

- **Protected Health Information.** Anthem's nine categories include: identity data, provider data, claims Payment information, member financial data, clinical claims data, medical record data, premium information, operational claim data, and product data), including Summary Health and Limited Data Sets, and
- **Protected Financial Information.** As a general rule, Protected Financial Information is treated the same as Protected Health Information.

cryptographic controls: Controls used to protect information by converting it into indecipherable data. See Encryption for more information.

Data at Rest: Data in computer storage. Data that falls under this category could include files stored on a company's local hard drive, copies of the file stored on onsite and offsite backup media and files on the servers of the storage area network (SAN).

Data in Transit: Data being transferred between two nodes in a network. It is data that is exiting the network via email, web, or other Internet protocols. Removable media carried from one location to another could be considered data in transit.

Data in Use: Data that temporarily resides in computer memory to be read or updated by a database or application.

degauss: A process used only on magnetic media which reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing, renders the drive permanently unusable.

Email and Messaging Systems: Email and Messaging systems refers collectively to: Email, Instant messaging and chat systems, text messaging systems (such as SMS, MMS, TMS, BBM, iMessage, etc.), video conferencing systems, teleconferencing systems (including telephone-based systems such as InterCall Reservationless-Plus and Voice Over IP (VoIP) systems such as Skype or Google Voice), social media systems (such as Facebook, Twitter, LinkedIn, Yammer, Blogger, YouTube, Flickr, Wikipedia, etc.) or the corporate accounts and pages established on those systems.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

external transmission: The communication of Anthem information to any person or entity where the communication media extends beyond the internal Anthem network

firewall: A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.

Foundation Series Documents: The policies, programs, standards, guidelines, and procedures that enact the WISP and further describe the intent of the policy statements.

guideline: Provides a recommendation of what should be done and how, to achieve the objectives set out in a security policy.

hybrid cloud: An integrated cloud computing platform that combines the potential of both public and private clouds. They provide some of the flexibility of public clouds, and some of the controls of private clouds. See *cloud computing*, *private cloud* and *public cloud* for more information.

incinerate: The act of burning completely to ashes.

Information Classification: The allocation of information assets into one of a series of categories and the application of specific controls based on those categories.

Information Security: The corporate Anthem security program that encompasses policy, operations, and the Office of the Chief Information Security Officer.

Information Security Standards Manual (ISSM): Provides a description of the minimum requirements that must be met to maintain compliance with security policy. ISSMs are generally based upon role or are technology agnostic.

information system: Information Systems refer to the technology used for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information Systems also include specialized systems such as telephone switching/private branch exchange (PBX) systems and environmental control systems.

integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

internal hard drives: Hard drives within Information Systems used for the storage of information. Typically these include hard drives within workstations, laptops, servers, copy machines, network appliances, or other devices.

laptop computers: Mobile Computing Devices which utilize the primary components of a traditional desktop computer to enable the user to access and/or store company data, include a full desktop operating system such as Microsoft Windows, Mac OS X, or Red-hat Linux, and afford IT staff full administrative control over the device and operating system.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

Limited Distribution (data classification): Any information intended solely for use by workforce members when conducting Anthem business. Disclosure of this information requires discretion upon its distribution so only those with a business need-to-know have access to it. Limited Distribution information is often described as "Internal Use Only." Differs from Confidential Information in that it does not include any individually identifiable information, nor does it include any proprietary Anthem information that could cause serious harm to the company if disclosed in error. If released or disclosed without authorization may have a limited impact on the organization or internal operations.

mail: Includes, but is not limited to: Mail shipments through the U.S. Postal Service., Shipments using a common carrier, such as FedEx or UPS.

media: Includes Internal Hard Drives, Non-digital Media, Removable Media, and Tapes.

merchant: Any entity that accepts payment cards bearing the logos of any of the five members of PCI Security Standards Council (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

Mobile Communications or Convergence Devices: Mobile Computing Devices which enable the user to access and/or store company data, but do not run a full desktop operating system and allow diminished administrative control of the device and operating system to IT staff. Examples of such devices include, but are not limited to, personal media players, cellular telephones, digital cameras, audio recording devices, e-Book Readers, tablet computers, iPhones, iPads, Android devices, Blackberry devices, and webOS devices.

Mobile Computing Devices (or "Mobile Devices"): Includes both Laptop Computers and Mobile Communications or Convergence Devices.

multifactor authentication (MFA): Multifactor authentication refers to the method of authentication that requires more than one factor before a user will gain access to a network or system. These factors may be a combination of something the User knows (e.g., passwords), something they own (e.g., hardware token), or something they are (e.g. fingerprint, biometrics, etc.). For example, use of a security token (a physical device such as a special smart card) together with something the user knows, such as a PIN or a password, would constitute the use of multifactor authentication.

multi-tenancy: Multi-tenancy refers to the shared use of hardware, software, resources and/or personnel by multiple consumers, potentially belonging to different organizations.

Non-digital Media: Media used to store non-digital information. Examples include hardcopy, microfilm and microfiche.

patch management: The process of reviewing and deploying on a timely basis approved software patches which mitigate Information System security flaws or vulnerabilities.

Policy: High-level documents that represent Anthem's overall Information Security intention and direction as formally expressed by the Chief Information Security Officer and senior management.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

Primary Account Number (PAN): Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account, also referred to as "account number."

private cloud: Provided as a cloud computing-based service over a dedicated network link. Private cloud arrangements offer the client the most control over underlying technology infrastructure, and less multi-tenancy than public clouds. Typically, private cloud models are more expensive than other options. Private cloud environments can be designed for specific scenarios. This type of service is the most desirable solution for the storage of Confidential Information. See Cloud Computing Security for more information.

Privileged Account: An account that is correlated to an end-user and is authorized to perform critical system privileged relevant functions that ordinary users are not authorized to perform.

Procedure: Provides a step-by-step description of how to implement the intent of a security policy as it applies to a specific, repeatable business process.

Programs: Documents that define the required governance, structure, workflow and communications for successfully implementing the program and state requirements for defining, assessing and monitoring program compliance.

Protected Financial Information: Non-public information about an Individual that the Individual provides to Anthem to obtain an insurance product or service from Anthem; information about an Individual resulting from a transaction involving an insurance product or service between Anthem and the Individual; or information Anthem otherwise obtains about an Individual in connection with providing an insurance product or service to that Individual.

Public (data classification): Refers to any information that has been released to the public by authorized management or is readily available to the public (such as through news services or the Internet). If released or disclosed would have no impact on the organization, our customers or business operations.

public cloud: Provided as a cloud computing-based service typically over the Internet with little or no control over the underlying technology infrastructure. This is the least expensive model of delivery that leverages the largest level of multi-tenant architecture. This service provides the fewest Information Security controls to mitigate risk and is not desirable for storage of Confidential Information without additional external controls. See Cloud Computing Security for more information.

pulverize: The act of grinding to a powder or dust.

Removable Media: Any media that are being used for the physical transportation or offline storage of information. Examples include: USB flash drives, compact flash cards, eSATA removable drives, Firewire connected devices, memory cards, Thunderbolt storage devices (MAC OSX only), and Media Transfer Protocol (MTP) devices.

shred: The act of cutting or tearing into small particles. The shred size of the refuse must be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

Standard: Provides a description of the minimum requirements that must be met to maintain compliance with security policy. ISSMs and Technical Configuration Standards are types of Standards.

tapes: Magnetic tape media used for the storage of digital information. Tapes are used most frequently for the long term storage of data.

Technical Configuration Standard (TCS): Specifies the baseline security requirements necessary to harden corporate information systems and information resources. These requirements are based on WISP policies and standards, and on industry best practices. Technical Configuration Standard (TCS) documents are directed at specific technologies and are limited to security configuration settings.

vaulting: A method of securely storing, managing, and tracking the use of privileged credentials

vendor: Any person or entity that receives, maintains, processes or otherwise is permitted access to Anthem systems or data through its provision of services directly to Anthem.

vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

wipe: Software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk drive or other digital media.

workforce members: Workforce members refer to Anthem associates, volunteers, trainees, temporary workers, consultants and contractors, and other persons whose conduct, in the performance of work for Anthem, is under the direct control of Anthem, whether or not they are paid by Anthem.

Anthem

Information Security Program

Title:	**Anthem Workforce Information Security Program Overview**		
Classification:	**Limited Distribution**	**Version No.**	**1.6**
Owner:	**Chief Information Security Officer**	**Last Annual Review:**	**01/28/2019**

3.2 Acronyms

ACH	Automated Clearing House
CISO	Chief Information Security Officer
EFT	Electronic Funds Transfer
ELT	Executive Leadership Team
ePHI	Electronic Protected Health Information
ESG	Enterprise Standards Governance
FACTA	Fair and Accurate Credit Transaction Act
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HITECH Act	Health Information Technology for Economic and Clinical Health Act
IM	Instant Message
ISSM	Information Security Standards Manual
NPI	Nonpublic Personal Information
PAN	Primary Account Number
PIN	Primary Identification Number
PBX	Private Branch Exchange
PCI-DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
PHI	Protected Health Information
PII	Personally Identifiable Information
SLT	Senior Leadership Team
TCS	Technical Configuration Standard
WISP	Anthem Workforce Information Security Program

4 - Security Program Review Cycle

At a minimum, all security program documents will be reviewed on an annual basis or as changes are made to address changing vulnerabilities and to ensure compliance with changing regulatory requirements.

HITRUST

Letter of Certification

August 26, 2018

Anthem, Inc.
120 Monument Circle
Indianapolis, IN 46204

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved HITRUST CSF Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST CSF Assurance Program, the following system of the organization meets the HITRUST CSF v9.1 Certification Criteria:

Anthem, Inc. - Government Business – Claims (Facets)

The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time
- No data security breach reportable to a federal or state agency by law or regulation has occurred
- No significant changes in the business or security policies, practices, controls and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria
- Annual progress is being made on areas identified in the Corrective Action Plan (CAP)
- Timely completion of the interim review as defined in the HITRUST CSF Assurance Program Requirements

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information security tailored to the healthcare industry. With input from leading organizations within the industry, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For those HITRUST CSF control requirements that are not currently being met, the organization must have a CAP that outlines its plans for meeting such requirements.

HITRUST performs a quality assurance review consistent with the HITRUST CSF assurance program requirements to ensure that the scores are consistent with the testing performed by the HITRUST CSF Assessor organization.

A full copy of the certification report has also been issued to the organization listed above. This full report includes additional details on the scope of the assessment, a representation letter from management, testing results for those controls required for certification, a benchmark report comparing the organization's results to industry results, details on CAPs required for

HITRUST CSF certification, and the completed questionnaire. If interested in obtaining a copy of the full report, you will need to contact the organization directly.

Additional information on the HITRUST CSF Certification program can be found at the HITRUST website: www.hitrustalliance.net.

HITRUST