SOC 2® + HITRUST Illustrative Report

The AICPA has developed an illustrative report to assist CPAs in reporting on the fairness of the presentation of a description of a service organization's system relevant to security, availability and confidentiality, and the suitability of the design and operating effectiveness of controls over those aspects of the system based on

(1) the criteria for the security, availability, and confidentiality principles included in the AICPA Trust Services Principles and Criteria *for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2014) (applicable trust services criteria) and

(2) the requirements in Health Information Trust Alliance Common Security Framework (HITRUST CSF).

This engagement is performed under AT section 101, *Attest Engagements* (AICPA, *Professional Standards*), to enable service organizations to provide information to users of the service organization's system about whether controls at the service organization relevant to security, availability, and confidentiality are suitably designed and operating effectively to meet the applicable trust services criteria and the HITRUST CSF requirements. This enables the service organization to communicate information about the processes and procedures it uses to meet the HITRUST CSF in addition to the applicable trust services criteria, increasing transparency and providing information for decision making.

Paragraph 1.33 of AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* specifies the components of a SOC 2 report[1] and the information to be included in each component, but the paragraph does not specify the format for these reports. Service organizations and service auditors may organize and present the required information in a variety of formats. The format of the type 2 SOC 2 report presented in this document is meant to be illustrative rather than prescriptive. The illustrative report contains all of the components of a type 2 SOC 2 report; however, for brevity, it does not include everything that might be described in a type 2 SOC 2 report. Ellipses (...) or notes to readers indicate places where detail has been omitted.

The trust services principle(s) addressed by the report, the controls specified by the service organization, and the tests performed by the service auditor are presented for illustrative purposes only in the illustrative reports. They are not intended to represent the principles that would be addressed in every type 2 SOC 2 engagement or the controls (or tests of controls) that would be appropriate for all service organizations. The trust services principles addressed by the report, the controls a service organization would include in its description, and the tests of controls a service auditor would perform for a specific type 2 SOC 2 engagement will vary based on the specific facts and circumstances of the engagement. Accordingly, it is expected that actual type 2 SOC 2 reports will address different principles and include different controls and tests of controls that are tailored to the service organization and the system that is the subject of the engagement.

[1] The components of a SOC 2 report are the service auditor's report, management's assertion, management's description of the service organization's system, and (in a type 2 SOC 2 report) a description of the service auditor's tests of the operating effectiveness of controls and the results of those tests.

In the illustrative reports, HITRUST CSF version 7 is the source of the HITRUST CSF requirements. HITRUST periodically issues new requirements. Accordingly, the practitioner's report and management's assertion should indicate the version of the HITRUST CSF that has been used when identifying the requirements.

The AICPA periodically issues new trust services principles and criteria. Accordingly, the practitioner should identify the version of the trust services principles and criteria used in performing the engagement. Also, management's assertion and the service auditor's report should indicate the version of the trust services principles and criteria used when identifying the criteria.

PART 1—ILLUSTRATIVE REPORT

In the following illustrative type 2 SOC 2 report, the service auditor is reporting on

- the fairness of the presentation of the service organization's description of its system based on the description criteria identified in management's assertion and
- the suitability of the design and operating effectiveness of its controls relevant to security, availability, and confidentiality based on the criteria for security, confidentiality, and availability in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) and the suitability of the design and operating effectiveness of its controls in meeting the requirements in the HITRUST CSF.

CONTENTS

Section 1—Management of Example Health Care Organization's Assertion Regarding Its PDR System Throughout the Period January 1, 20X1, to December 31, 20X1

We have prepared the description titled, "Example Health Care Organization's Description of Its PDR System Throughout the Period January 1, 20X1, to December 31, 20X1," (description), based on the criteria for a description of a service organization's system identified in paragraphs 1.26–1.27 of AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the PDR System, particularly system controls intended to meet the criteria for the security, availability, and confidentiality principles (applicable trust services criteria) set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*), and the requirements set forth in the HITRUST CSF version 7 (HITRUST CSF requirements).

The organization is classified as a Health Care Insurance Payor covering 20 million members; applicable HITRUST requirements have been determined based on the characteristics of the entity described in subsection XXX of the description.[2]

We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the PDR System throughout the period January 1, 20X1, to December 31, 20X1, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are as follows:

(a) **Infrastructure.** The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks)

(b) **Software.** The application programs and IT system software that support application programs (operating systems, middleware, and utilities)

(c) **People.** The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers)

(d) **Procedures.** The automated and manual procedures

(e) **Data.** Transaction streams, files, databases, tables, and output used or processed by the system)

(3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

[2] The HITRUST CSF follows a risk-based approach and therefore applies security resources commensurate with the level of risk or as required by applicable regulations or standards. HITRUST addresses risk by defining multiple levels of implementation requirements. The implementation requirement levels relate to the degree of restrictiveness for a particular control. Three levels of requirements are defined based on organizational, system, or regulatory risk factors. Level 1 is the minimum set of security requirements for all systems and organizations regardless of size, sophistication, or complexity. Levels 2 and 3 are required only for organizations and systems of increased risk and complexity as determined by the associated organization, system, and regulatory factors of the service organization. The information presented here is meant to be illustrative and will change based on the risk factors.

(5) The process used to prepare and deliver reports and other information to user entities or other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, (*a*) how such information is provided or received and the role of the subservice organization and other parties and (*b*) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

(9) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore.

(10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were those necessary to meet the applicable trust services criteria and the HITRUST CSF requirements.

c. the controls stated in the description, which together with the complementary user entity controls referred to above if suitably designed, were suitably designed throughout the period January 1, 20X1, to December 31, 20X1, to meet the applicable trust services criteria and the HITRUST CSF requirements.

d. the controls stated in the description, which together with the complementary user entity controls referred to above if operating effectively, operated effectively throughout the period January 1, 20X1, to December 31, 20X1, to meet the applicable trust services criteria and the HITRUST CSF requirements.

Section 2—Independent Service Auditor's Report

Independent Service Auditor's Report

To Example Health Care Organization

Scope

We have examined the description titled "Example Health Care Organization's Description of its PDR System Throughout the Period January 1, 20X1, to December 31, 20X1" (description) based on the criteria set forth in paragraphs 1.26–1.27 of AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability, and confidentiality principles set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria), throughout the period January 1, 20X1, to December 31, 20X1. We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the HITRUST CSF version 7 control specifications (HITRUST CSF requirements).

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of the service organization's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information in the section titled "Other Information Provided by Example Health Care Organization Not Covered by the Service Auditor's Report" (1) describes the HITRUST CSF implementation requirements, the segment specific HITRUST CSF requirements, and risk factors; (2) provides a mapping between the requirements in the HITRUST CSF version 7 and the equivalent applicable trust services criteria; and (3) includes a copy of Example Health Care Organization's CSF report issued by HITRUST. This information is presented by the management of Example Health Care Organization to provide additional information and is not a part of the service organization's description of its PDR System made available to user entities during the period from January 1, 20X1, to December 31, 20X1. This information has not been subjected to the procedures applied in the examination of the description of the PDR System and the suitability of the design and operating effectiveness of controls to meet the related applicable trust services criteria and HITRUST CSF requirements stated in the description of the PDR System, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

Example Health Care Organization has provided its accompanying assertion titled "Management of Example Health Care Organization's Assertion Regarding its PDR System Throughout the Period January 1, 20X1, to December 31, 20X1," regarding the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria and the HITRUST CSF requirements. Example Health Care Organization is responsible for (1) preparing the description and the assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria and the HITRUST CSF requirements from being met; (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria and the HITRUST CSF requirements; and (6) specifying the controls that meet the applicable trust services criteria and the HITRUST CSF requirements and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the

- fairness of the presentation of the description based on the description criteria; and

- suitability of the design and operating effectiveness of the controls to meet both the applicable trust services criteria and the HITRUST CSF requirements, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria and HITRUST CSF requirements throughout the period January 1, 20X1, to December 31, 20X1.

Our examination involved performing procedures to obtain evidence about (1) the fairness of the presentation of the description based on the description criteria and (2) the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria and HITRUST CSF requirements. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria and HITRUST CSF requirements. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria and HITRUST CSF requirements were met. Our examination also included evaluating the overall presentation of the description, the suitability of the controls objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria and HITRUST CSF requirements. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria and HITRUST CSF requirements is subject to risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria and HITRUST CSF requirements,

a. the description fairly presents the system that was designed and implemented throughout the period January 1, 20X1, to December 31, 20X1;

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria and HITRUST CSF requirements would be met if the controls operated effectively throughout the period January 1, 20X1, to December 31, 20X1, and user entities applied the complementary user entity controls contemplated in the design of the Service Organization's controls throughout the period January 1, 20X1, to December 31, 20X1; and

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria and HITRUST CSF requirements were met, operated effectively throughout the period January 1, 20X1, to December 31, 20X1.

Description of Tests of Controls

The specific controls tested, the tests performed, and results of those tests are presented in the section titled, "Applicable Trust Services Criteria, HITRUST CSF Requirements, Example Health Care Organization's Related Controls, and Service Auditor's Tests of Controls and Results."

Restricted Use

This report, including the description of tests of controls and results thereof as presented in section IV, is intended solely for the information and use of Example Health Care Organization; user entities of Example Health Care Organization's PDR System during some or all of the period January 1, 20X1, to December 31, 20X1; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities or other parties
- Internal control and its limitations
- The applicable trust services criteria and HITRUST CSF requirements
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria and HITRUST CSF requirements.
- The risks that may threaten the achievement of the applicable trust services criteria and HITRUST CSF requirements and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

[*Service auditor's signature*]

[*Service auditor's city and state*]

[*Date of the service auditor's report*]

Section 3—Example Health Care Organization's Description of Its PDR System Throughout the Period January 1, 20X1, to December 31, 20X1

For examples of information that would be included in this section of a type 2 report, see section 3 of the illustrative type 2 service organization controls report in appendix D of the AICPA SOC 2® guide.

Additional HITRUST considerations:

HITRUST CSF implementation / segment specific requirements and risk factors

Simple description of the characteristics (for example, Segment and Risk Factors) of the entity and determining factors. Based on the following characteristics of "Example Health Care Organization's" services and its system, the applicable HITRUST CSF requirements have been determined….

Section 4—Applicable Trust Services Criteria, HITRUST CSF Requirements, Example Service Organization's Related Controls, and Service Auditor's Tests of Controls and Results

Note to Readers:

The source of the criteria used in this document is

1. *the 2014 version of the AICPA* Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP section 100) *and*

2. *version 7 of the HITRUST CSF.*

Although the applicable trust services criteria and related controls are presented in this section, they are, nevertheless, an integral part of Example Health Care Organization's description of its PDR system throughout the period January 31, 20X1, to December 31, 20X1. This type 2 SOC 2 report is for illustrative purposes only and is not meant to be prescriptive. Example Health Care Organization's controls and test of controls presented in this section are for illustrative purposes and accordingly are not all inclusive and may not be suitable for all service organizations and examinations.

The matrix in exhibit 1 presents information about a service organization's controls, the service auditor's tests of controls, and the results of those tests. Column 1 of the matrix identifies the HITRUST implementation requirement level and column 2 identifies the trust services criteria that are equivalent to the HITRUST requirement shown in column 3. The format and organization of the information is not prescribed and may vary based on user needs.

Exhibit 1. Applicable Trust Services Criteria, HITRUST CSF Requirements, Example Service Organization's Related Controls, and Service Auditor's Tests of Controls and Results

1	2	3	4	5	6
HITRUST CSF (Level)	**TSPC**	**HITRUST Baseline Requirement Statement (Control Statement)**	**Management of Example Service Organization's Control**	**Service Auditor's Tests of Controls**	**Results of Tests**
09.m (1)	CC5.1 CC5.6 CC5.7 A1.1 A1.2	Wireless access points are configured with strong encryption (WPA at a minimum) and are placed in secure locations.	Wireless access points are located and configured in accordance with documented policies and procedures. Configuration and location quality checks are performed to confirm (*a*) default keys and passwords are changed, (*b*) other settings are accurately configured, and (*c*) wireless access points are placed in secure locations.	Inspected the wireless configurations and locations for a sample of access points to determine whether access was configured in accordance with documented policies and procedures. Inspected documentation evidencing the	

1	2	3	4	5	6
HITRUST CSF (Level)	**TSPC**	**HITRUST Baseline Requirement Statement (Control Statement)**	**Management of Example Service Organization's Control**	**Service Auditor's Tests of Controls**	**Results of Tests**
				completion of a sample of configuration and location quality checks.	
09.m (1)	CC5.1 CC5.6 CC5.7 A1.1 A1.2	Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.	Wireless access points are located and configured in accordance with documented policies and procedures. Configuration quality checks are performed to confirm vendor defaults and passwords are changed prior to implementation of the access point.	For a sample of wireless access point implementations, inspected evidence of authorization and modification of vendor defaults. Inspected documentation evidencing the completion of a sample of configuration quality checks.	
09.m (1)	CC5.1 CC5.6 CC5.7 A1.1 A1.2	A current network diagram (including wireless networks) exists and is updated whenever there are network changes and no less than every 6 months.	Management reviews and approves the network diagram each quarter. Requested modifications are tracked, approved, and implemented.	Inspected documentation evidencing the completion of a sample of network diagram reviews performed by management.	
09.m(2)	CC5.1 CC5.6 CC5.7 A1.1 A1.2	Firewall, router, and network connection changes are approved and tested prior to implementing the changes.	Management monitors changes made to firewalls, routers, and network connections monthly. Management inspects approval and testing documentation for a sample of firewall, router, and network connection changes and confirms that approval and testing occurred prior to implementing the changes.	For a sample of months, inspected documentation evidencing the completion of the firewall, router, and network connection change monitoring executed by management. For a sample of changes validated by management, inspected the change	

1	2	3	4	5	6
HITRUST CSF (Level)	**TSPC**	**HITRUST Baseline Requirement Statement (Control Statement)**	**Management of Example Service Organization's Control**	**Service Auditor's Tests of Controls**	**Results of Tests**
				tickets to determine whether the changes were approved and tested prior to implementation.	
09.m(3)	CC5.1 CC5.6 CC5.7 A1.1 A1.2	Quarterly networks scans are performed to identify unauthorized components and devices.	ABC organization completes quarterly network scans to identify unauthorized components and devices.	Inspected the network scan for a sample of quarters to determine whether the network scan was completed and included unauthorized components and devices.	

[Note: See explanation of level included in section V)

The matrix in exhibit 2 illustrates another format for presenting information about a service organization's controls, the service auditor's tests of controls, and the results of those tests. In this matrix, the shaded row identifies the trust services criterion. Beneath that row, column 1 of the matrix identifies the HITRUST implementation requirement level and column 2 identifies the HITRUST CSF requirement that is equivalent to the trust services criteria shown in the shaded row. The matrix in exhibit 2 includes only a sample of CSF requirements for illustrative purposes; actual reports will include all of the CSF requirements that map to the applicable trust services criteria.

Exhibit 2. Applicable Trust Services Criteria, HITRUST CSF Requirements, Example Service Organization's Related Controls, and Service Auditor's Tests of Controls and Results

CC5.0—Logical and Physical Access Controls: The entity has placed security controls against unauthorized access (both physical and logical). CC5.1—Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.			
HITRUST CSF (Level)	**CSF Baseline Requirement Statement (Control Statement)**	**Management of Example Service Organization's Control**	**Service Auditor's Tests of Controls and Results**
01.b (1)	User identities are verified prior to establishing accounts.	A New User Approval Form is completed by the new hire. The form is then reviewed and approved by his or her department manager prior to establishing the account.	For a judgmental selection of new hires, obtained the New User Approval Form and confirmed it was reviewed and approved by their department manager prior to the account being established.
01.b (1)	Default and unnecessary system accounts are removed, disabled, or otherwise secured. (For example, the passwords are changed and privileges are reduced to the lowest levels of access.)	A semi-annual system account review is conducted to support that all default and unnecessary system accounts are removed, disabled, or otherwise secured. (For example, the passwords are changed and privileges are reduced to the lowest levels of access.)	For one of the system account reviews, ascertained that all system accounts were reviewed and where modifications were identified, were resolved on a timely basis.

CC5.0—Logical and Physical Access Controls: The entity has placed security controls against unauthorized access (both physical and logical). CC5.1—Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.			
HITRUST CSF (Level)	**CSF Baseline Requirement Statement (Control Statement)**	**Management of Example Service Organization's Control**	**Service Auditor's Tests of Controls and Results**
01.b (1)	Account managers are notified when users' access rights change (for example, termination, change in position) and modify the users account accordingly.	A Modified User Access Approval Form is completed by the user's supervisor. The form is reviewed and approved by the department manager prior to modifying the user's account access establishing the account. A semi-annual system account review is conducted.	For a sample of modified user accounts, inspected the Modified User Access Form and confirmed it was reviewed and approved by the department manager prior to modifying the user account access. For a sample of semi-annual account reviews, determined through inspection of documentation and system files that access was reviewed and a sample of requested modifications were resolved accurately and timely.

CC5.0—Logical and Physical Access Controls: The entity has placed security controls against unauthorized access (both physical and logical). CC5.1—Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.			
HITRUST CSF (Level)	**CSF Baseline Requirement Statement (Control Statement)**	**Management of Example Service Organization's Control**	**Service Auditor's Tests of Controls and Results**
01.b (1)	User registration and de-registration, at a minimum, communicates relevant policies to users and requires signed acknowledgement, checks authorization and minimum level of access necessary prior to granting access, ensures access is appropriate to the business or clinical needs (or both) (consistent with sensitivity or risk and does not violate segregation of duties requirements), addresses termination and transfer, ensures default accounts are removed or renamed (or both), removes or blocks critical access rights of users who have changed roles or jobs, and automatically removes or disables inactive accounts.	A New User Approval Form is completed by the new hire. The form is then reviewed and approved by the department manager prior to establishing the account. A Modified User Access Approval Form is completed by the user's supervisor. The form is reviewed and approved by the department manager prior to modifying the user's account access establishing the account. A semi-annual system account review is conducted.	For a judgmental selection of new hires, obtained the New User Approval Form and confirmed it was reviewed and approved by the department manager prior to the account being established. For a sample of modified user accounts, inspected the Modified User Access Form and confirmed it was reviewed and approved by the department manager prior to modifying the user account access. For a sample of semi-annual account reviews, determined through inspection of documentation and system files that access was reviewed and a sample of requested modifications were resolved accurately and timely.
01.b (1)	Users are given a written statement of their access rights, which they are required to sign stating they understand the conditions of access.	As part of the new hire orientation, employees need to sign a User Agreement prior to receiving their access badge and online credentials.	For a judgmental selection of new hires, obtain the signed User Agreement and confirm it was signed prior to begin granted access.

CC5.0—Logical and Physical Access Controls: The entity has placed security controls against unauthorized access (both physical and logical). CC5.1—Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.			
HITRUST CSF (Level)	**CSF Baseline Requirement Statement (Control Statement)**	**Management of Example Service Organization's Control**	**Service Auditor's Tests of Controls and Results**
01.c (1)	Privileges are formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their function role, and documented for each system product or element.	User access to the System is authorized and documented by the user's manager via an access request form. Access is provisioned through role based access dependent on the user's job function.	For a judgmental selection of new and changed user access requests during the specified period, verified that access was authorized by the employee's manager through inspection of access request forms for each user. Further, verified that role-based access allocated to each selected access change was appropriate based on the user's job function.
01.c (1)	The organization explicitly authorizes access to specific security relevant functions (deployed in hardware, software, and firmware) and security-relevant information.	User access to security administration rights and security information related to hardware, software, and firmware supporting the system is authorized and documented by the user's manager via an access request form.	For a judgmental selection of new and changed administrative user access requests during the specified period, verified that access was authorized by the employee's manager through inspection of access request forms for each user.
Additional CSF per mapping.			

Section 5—Other Information Provided by Example Health Care Organization Not Covered by the Service Auditor's Report

Subsection: HITRUST CSF implementation / segment specific requirements and risk factors

Implementation Requirement Levels
The HITRUST CSF follows a risk-based approach and therefore applies security resources commensurate with level of risk or as required by applicable regulations or standards. HITRUST addresses risk by defining multiple levels of implementation requirements. The implementation requirement levels relate to the degree of restrictiveness for a particular control. Three levels of requirements are defined based on organizational, system, or regulatory risk factors. Level 1 is considered the baseline level of control requirements as determined by the industry; each subsequent level encompasses the lower levels and includes additional requirements commensurate with increased risk. [1]

Segment Specific Requirements
Certain industry segments have specific requirements that do not apply to other segments or would not be considered reasonable and appropriate from a general controls perspective. For example, the HITRUST CSF contains a CMS Contractors category which outlines additional controls and requirements that contractors of CMS will need to implement in addition to those controls listed in the Implementation Requirement Levels. An example of this would be requiring specific authorization or approval from the CMS CIO. New for 2015 are segment-specific requirements for Health Insurance Exchanges (HIXs) and Federal Agencies and Contractors.

Risk Factors
The HITRUST CSF defines a number of organizational, system, and regulatory risk factors that increase the inherent risk to an organization or a system, necessitating a higher level of control.

- **Organizational Factors:** The organizational factors are defined based on the size of the organization and complexity of the environment as follows:
  - Volume of business
    - Health Plan and Insurance—Number of Covered Lives
    - Medical Facilities and Hospital—Number of Licensed Beds
    - Pharmacy Companies—Number of Prescriptions Per Year
    - Physician Practice—Number of Visits Per Year
    - Third Party Processor—Number of Records Processed Per Year
    - Biotech Companies—Annual Spend on Research and Development
    - IT Service Provider and Vendor—Number of Employees
    - Health Information Exchange—Number of Transactions Per Year
  - Geographic scope
    - State
    - Multi-state
    - Off-shore (outside U.S.)
    -
- **Regulatory Factors:** The regulatory factors are defined based on the compliance requirements applicable to an organization and systems in its environment:
  - Subject to PCI Compliance
  - Subject to FISMA Compliance
  - Subject to FTC Red Flags Rules
  - Subject to the State of Massachusetts Data Protection Act
  - Subject to the State of Nevada Security of Personal Information Requirements
  - Subject to the State of Texas Medical Records Privacy Act

- Subject to Joint Commission Accreditation
- Subject to CMS Minimum Security Requirements (High-level Baseline)
- Subject to MARS-E Requirements
- Subject to FTI Requirements

- **System Factors:** The system factors are defined considering various system attributes that would increase the likelihood or impact of a vulnerability being exploited. These factors are to be assessed for each system or system grouping to determine the associated level of control.
    - Stores, processes, or transmits PHI
    - Accessible from the Internet
    - Accessible by a third party
    - Exchanges data with a third party or business partner
    - Publicly accessible
    - Mobile devices are used
    - Connects with or exchanges data with a Health Information Exchange (HIE)
    - Number of interfaces to other systems
    - Number of users
    - Number of transactions per day

For a system to increase from a Level 1 Implementation Requirement to a Level 2 or 3 Implementation Requirement, the system must be processing ePHI and include at least one of the other system factors associated with the control. For example, if a system is accessible from the Internet, exchanges data with a business partner, and has the Level 2 threshold number of users, but does not process ePHI, that system is only required to meet the Level 1 Implementation Requirements. However, if another system does process ePHI and is accessible from the Internet, then that system must meet an Implementation Requirement level higher than Level 1.

Section 5 (continued)—Other Information Provided by Example Health Care Organization Not Covered by the Service Auditor's Report

Subsection: Mapping between the HITRUST CSF version 7 and the Trust Services Principles and Criteria

Criteria		HITRUST Common Security Framework (CSF)					
A1.0	Additional Criteria for Availability	00 a	01 a	01 b	09 l	09 m	09 n
A1.1	Current processing capacity and usage are maintained, monitored and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.					X	
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.					X	
A1.3	Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.						
Criteria							
CC5.0	Common Criteria Related to Logical / Physical Access Controls						
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.					X	
CC5.2	New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.						
CC5.3	Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).						
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.						
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.						
CC5.6	Logical access security measures have been implemented to protect against security, availability and confidentiality threats from sources outside the boundaries of the system.					X	
CC5.7	The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security, availability and confidentiality.					X	
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.						

Section 5 (continued)—Other Information Provided by Example Health Care Organization Not Covered by the Service Auditor's Report

Subsection: HITRUST CSF certification report

Sample of HITRUST CSF Certification Report (PDF Link)

PART 2—ILLUSTRATIVE MANAGEMENT ASSERTION AND SERVICE AUDITOR'S REPORT WHEN COMPLMENTARY USER ENTITY CONTROLS ARE NECESSARY TO ACHIEVE THE CRITERIA

Language shown in ***boldface italics*** represents modifications that would be made to the service auditor's report if complementary user-entity controls are needed to meet certain applicable trust services criteria.

ILLUSTRATIVE MANAGEMENT ASSERTION (Type 2) WHEN COMPLMENTARY USER ENTITY CONTROLS ARE NECESSARY TO ACHIEVE THE CRITERIA

Section 1—Management of [*XYZ Service Organization's*] Assertion Regarding its System Throughout the Period [*date*] to [*date*]

We have prepared the description titled, "Description of [*XYZ Service Organization's*] [*type or name*] System throughout the period [*date*] to [*date*]," (description), based on the criteria for a description of a service organization's system identified in paragraph 1.26–1.27 of AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the [type or name] system, particularly system controls intended to meet the criteria for the security, availability, and confidentiality principles (applicable trust services criteria) set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria), and the requirements set forth in the HITRUST CSF version 7 (HITRUST CSF requirements[3]).

The organization is classified as [insert relevant risk factors for service organization]; applicable HITRUST CSF requirements have been determined by the characteristics of the entity described [in or on subsection/page X] of the description.

We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the [type or name] system throughout the period [*date*] to [*date*] based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are the following:

(a) **Infrastructure.** The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks)

(b) **Software.** The application programs and IT system software that supports application programs (operating systems, middleware, and utilities)

(c) **People.** The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers)

(d) **Procedures.** The automated and manual procedures

[3] The HITRUST CSF requirements constitute suitable criteria, as defined in paragraph 24 of AT 101, *Attest Engagements* (AICPA, *Professional Standards*). Omission of one or more of the criteria is likely to result in criteria that are not suitable because they are not complete. HITRUST periodically issues new criteria. The practitioner should check the HITRUST website for current applicable criteria and identify the HITRUST CSF version being used as the criteria in management's assertion and the service auditor's report.

(e) **Data.** Transaction streams, files, databases, tables, and output used or processed by the system

(3) The boundaries or aspects of the system covered by the description

(4) How the system captures and addresses significant events and conditions

(5) The process used to prepare and deliver reports and other information to user entities or other parties

(6) If information is provided to, or received from, subservice organizations or other parties, (a) how such information is provided or received and the role of the subservice organization and other parties and (b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls[4]

(7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, (a) complementary user-entity controls contemplated in the design of the service organization's system and (b) when the inclusive method is used to present a subservice organization, controls at the subservice organization[5]

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

(9) Any applicable trust services criteria that are not addressed by a control at the service organization ***or a subservice organization*** and the reasons therefore

(10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

(11) Relevant details of changes to the service organization's system during the period covered by the description

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

---

[4] Certain description criteria may not be pertinent to a particular service organization or system. For example, a service organization may not use any subservice organizations or other parties to operate its system. Because the criteria in paragraphs 1.26–1.27 of the SOC 2® guide may not be readily available to report users, management of a service organization should include in its assertion all of the description criteria in paragraphs 1.26–1.27 of the SOC 2® guide. For description criteria that are not pertinent to a particular service organization or system, report users generally find it useful if management presents all of the description criteria and indicates which criteria are not pertinent to the service organization and the reasons therefore. Management may do so either in its system description or in a note to the specific description criteria. The following is illustrative language for a note to criteria that are not pertinent to the service organization or its system:

Example Health Care Organization does not use subservice organizations or other parties to operate its PDR system. Accordingly, our description does not address the criteria in items (a)(i)(6) and (a)(i)(8).

[5] See footnote 3.

b. the controls stated in the description were those necessary to meet the requirements set forth in the HITRUST CSF.

c. the controls stated in the description, ***which together with the complementary user entity controls referred to above if suitably designed,*** were suitably designed throughout the period [*date*] to [*date*] to meet the applicable trust services criteria and the HITRUST CSF requirements.

d. the controls stated in the description, ***which together with the complementary user entity controls referred to above if operating effectively,*** operated effectively throughout the period [*date*] to [*date*] to meet the applicable trust services criteria and the HITRUST CSF requirements.

ILLUSTRATIVE SERVICE AUDITOR'S REPORT WHEN COMPLMENTARY USER ENTITY CONTROLS ARE NECESSARY TO ACHIEVE THE CRITERIA

Independent Service Auditor's Report

To Management of [*XYZ Service Organization*]

Scope

We have examined the description titled "Description of [*XYZ Service Organization's*] System Throughout the Period [date] to [date]" (the description) based on the criteria set forth in paragraph 1.26 of AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security, availability, and confidentiality principles set forth in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) (applicable trust services criteria), throughout the period [date] to [date]. We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the HITRUST CSF version 7 control specifications (HITRUST CSF requirements).

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of the Service Organization's controls are suitably designed and operating effectively, along with related controls at the Service Organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.]

[If Section V is included, the following information also may be included in the opinion: The information in the section titled "Other Information Provided by *XYZ Service Organization* Not Covered by the Service Auditor's Report" (1) describes the HITRUST CSF implementation requirements, segment specific requirements and risk factors, (2) provides the mapping between the HITRUST CSF version 7 and the Trust Services Principles and Criteria, and (3) includes a copy of *XYZ Service Organization's* CSF report issued by HITRUST. This information is presented by the management of *XYZ Service Organization* to provide additional information and is not a part of the service organization's description of its system made available to user entities during the period from [date] to [date]. This information has not been subjected to the procedures applied in the examination of the description of the System and the suitability of the design and operating effectiveness of controls to meet the related applicable trust services criteria and HITRSUT CSF requirements stated in the description of the System, and accordingly, we express no opinion on it.

[*If this is a SOC 2 Report including a HITRUST Certification, Section V is required and the opinion may include the above language]*

Service Organization's Responsibilities

Example Health Care Organization has provided its accompanying assertion titled "Management of *XYZ Service Organization*'s Assertion Regarding its System Throughout the Period [date] to [date]," regarding the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria and the HITRUST CSF requirements. *XYZ Service Organization* is responsible for (1) preparing the description and the assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services principles and criteria and HITRUST CSF requirements from being met; (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria and the HITRUST CSF requirements; and

(6) specifying the controls that meet the applicable trust services criteria and the HITRUST CSF requirements and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the

- fairness of the presentation of the description based on the description criteria and
- suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria and suitability of the design and operating effectiveness of the controls to meet the HITRUST CSF requirements, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria and HITRUST CSF requirements throughout the period [date] to [date].

Our examination involved performing procedures to obtain evidence about (1) the fairness of the presentation of the description based on the description criteria and (2) the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria and HITRUST CSF requirements. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria and HITRUST CSF requirements. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria and HITRUST CSF requirements were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria and HITRUST CSF requirements. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria and HITRUST CSF requirements is subject to risks that the system may change or that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the description criteria and the applicable trust services criteria and HITRUST CSF requirements,

a. the description fairly presents the system that was designed and implemented throughout the period [date] to [date];

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria and HITRUST CSF requirements would be met if the controls operated effectively throughout the period [date] to [date]***, and user entities applied the complementary user entity controls contemplated in the design of the Service Organization's controls throughout the period [date] to [date]***; and

c. the controls tested, ***which together with the complementary user entity controls referred to in the scope paragraph of this report***, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria and HITRUST CSF requirements were met, operated effectively throughout the period [date] to [date].

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section titled, "Applicable Trust Services Principles, Criteria, and HITRUST CSF Requirements and Related Controls, Tests of Controls, and Results of Tests".

Restricted Use

This report, including the description of tests of controls and results thereof as presented in Section IV, is intended solely for the information and use of XYZ; user entities of *XYZ Service Organization's* [type or name] system during some or all of the period [date] to [date]; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities or other parties
- Internal control and its limitations
- The applicable trust services criteria and HITRUST CSF requirements
- *[If complementary user entity controls are required to meet certain trust principles criteria, include the following language*:] Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria and HITRUST CSF requirements.
- The risks that may threaten the achievement of the applicable trust services criteria and HITRUST CSF requirements and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

[*Service auditor's signature*]

[*Service auditor's city and state*]

[*Date of the service auditor's report*]