From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Information Identification and Classification Policy Overview

This classification policy prescribes a system for classifying, safeguarding, and declassifying Health Insurance Company (HIC) information, especially information subject to the Health Insurance Portability and Accountability Act (HIPAA). The healthcare industry is a sharing environment which allows doctors, practitioners, providers, and insurers find quality care for their patients. Many entities depend on the free flow of information to provide on-time care and payments. Nevertheless, to protect privacy, specific information regarding the patient/insured are maintained in confidence in order to protect against economic harm, embarrassment, and discrimination.

HIC Classification Policy is mandatory as it outlines protections for customers and patients demonstrating our commitment to HIPAA. The classification model is based on both Mandatory Access Control (MAC) for labeling information based on its secrecy level. From the MAC model, we can have a tiered system for information labels: HIPAA, PCI, and PII are placed in the "Restricted" level, other PII and organizational information at the "confidential" level, and all other unregulated information placed as "Public" for a total of three tiers. The classic MAC model prevents information leakage to public and unauthorized parties.

For internal information access, we use the ABAC model to provide smart security, performance, and administrative solutions. Technology has evolved the DAC model to Role Based Access Control (RBAC), and then transformed to Attribute Based Access Control (ABAC) currently used as best practice. ABAC is used by the latest technology such as MS Azure. The ABAC model provides for identification and classification of devices, identities, roles, and authorization for those specific devices and roles. Furthermore, departments can be segmented into organizational units (OU) to restrict access to data classified under the MAC model.

I. Classification

1.1 Standards

(a) Information may be originally under the terms this policy only if all of the following conditions are met:
(1) An original classification authority is classifying the information
(2) The information is owned by, produced by or for, or is under the control of HIC.
(3) The information pertains to one or more of the regulations, laws, standards listed in section 1.4 of the policy.
(4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.
(b) If there is significant doubt about the need to classify information, it shall not be classified. This policy rule does not:
(1) Change criteria or procedures for classification
(c) Classified information shall not be declassified automatically as a result of disclosure of identical or similar information
(d) The unauthorized disclosure of business partner information is presumed to cause damage to HIC.
(ISOO, 2009)

1.2 Classification Levels

(a) Information may be classified at one of the following three levels:
(1) "**Public**" shall be applied to information, for information that will not harm the organization if data is available internally or to the public.
(2) "**Confidential**" shall be applied to information, for data available only to authorized users.
(3) "**Restricted**" shall be applied to information, for data that may cause financial, legal, regulatory or reputational damage if disclosed or compromised (Nolan & Wilson, 2015).
(4) If there is significant doubt about the level of classification, is shall be classified at the confidential level.

1.3 Classification and Data Lifecycle

(a) Information categorized in accordance with section 1.2 shall be covered in it's data life cycle during:
(1) Creation: During creation, data MUST be classified. Classification should exist for all common storage areas.
(2) Access: Classification of data should correlate with separation of duties (SOD) to access data.
(3) Use: Safeguarding and labeling data after its access according to its classification.
(4) Transmission: Transmitted in accordance with policies and standards (e.g. HIPAA, PCI DSS)
(5) Storage: Storage devices must be approved to protect non-public classified data and in accordance to industry defined standards.

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

(6) Physical Transport: Transport of data must be approved to protect non-public classified data and in accordance to industry defined standards (e.g. encrypted disks).
(7) Destruction: Information must be disposed in a controlled procedure. The standards that govern disposal of non-public classified data must ensure that data cannot be reconstructed.
(Johnson, 2015)

1.4 Classification Authority
(a)The authority to classify information may be exercised by:
(1) Chief Security Officer (CISO) or;
(2) by appointment of the CISO or CIO
(b) All classifications exercised by the CISO must first be approved by the:
(1) Chief Information Officer (CIO)

1.5 Classification Purpose
(a) Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable and describable damage to HIC in accordance with 1.2 of this order, as it pertain to one or more of the following laws, regulations, and auditable standards and controls specified by:

(1) Health Insurance Portability and Accountability Act (HIPAA)
(2) Sarbanes-Oxley Act (SOX)
(3) The Patient Protection and Affordable Care Act (ACA)
(4) Payment Card Information Data Security Standard (PCI DSS)
(5) National Association of Insurance Commissioners' ("NAIC") Model Acts
(6) The European General Data Protection Regulation (GDPR)
(7) Emerging laws and standards with high impact on HIC operations

1.6 Duration of Classification
(a) HIC classified information shall remain classified for the duration specified by State and Federal law.

1.7 Identification and Markings
(a) HIPAA: Information and documents relating to HIPAA must be handled and marked as described by HIPAA Rule and guidance on HHS.gov.
(b) PCI: Identification of payment card information (PCI) shall remain consistent with standards set by PCI Data Security Standards (PCI DSS).

1.8 Classification Prohibitions and Limitations
(a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:
(1) conceal violations of law, inefficiency, or administrative error
(2) prevent embarrassment to a person, organization, or agency
(3) restrain competition
(4) Prevent or delay the release of information that does not require protection in the interest of HIC.
(ISOO, 2009)

II. Declassification and Downgrading

2.1 HIPAA Related Deidentification (Downgrading)
(a) Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual (HHS.GOV, n.d.).

(b) As stated under HIPAA rules, de-identification shall occur with one of the two methods:
(a) "Expert Determination" method: A person with appropriate knowledge of and experience with generally accepted statistical and

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

scientific principles and methods for rendering information not individually identifiable.
(b) "Safe Harbor" method: The identifiers as described by HIPAA regarding the individual or of relatives, employers, or household members of the individual, are removed.
(HHS.GOV, n.d.).

2.2 Other De-identification and Downgrading of Data Classification
(a) Data of any type shall not be de-identified or downgraded in any other method or fashion than described in the HIC Policy, Federal or State Regulation, and without approval of the CIO.

III. Safeguarding

(a) A person may have access to classified information provided that:
(1) A favorable determination of eligibility for access have been made in accordance to HR policy
(2) the person has signed an approved nondisclosure agreement
(b) Users or future users of HIC information systems who meet the criteria in (a) of this section shall receive training to properly safeguard HIPAA, PCI, and consumer information and on the criminal and administrative penalties that may be imposed on an individual who fails to protect information from unauthorized disclosure.
(c) A user leaving HIC may nor remove HIC information from HIC control or direct that information to be downgraded as "public" in order to remove it from agency control.
(d) Information designated as "Restricted" or "Confidential" may not be physical moved or electronically transmitted outside of acceptable use policy and industry rules, standards, and regulations.
(e) The CISO, with or without collaboration with approved entities by the CIO or CEO, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed (i.e. "Data Lifecyle") under conditions that provide adequate protection and prevention access by unauthorized persons (ISOO, 2009).

IV. Implementation

AUTHORIZED OU (Organizational Unit)	DATA	DATA CATEGORY	ACCESS PURPOSE	RESTRICTIONS
•Claims •Workers Comp •Claims •Customer Services	Contact (individual) Financial (Income) Demographic (individual) Identification (individual)	**Confidential**	Analyze medical work performed with policy to disburse payment. Assist with customer questions regarding policy and eligibility.	No collection or unauthorized sharing of HIC customer information
•Claims Manager •Customer Services Manager	Financial (Bank Account) HIC Issued Info Government Issued ID Medical (aggregate) Personal (aggregate)	**Restricted**	Assist claims and customer services with issues requiring restricted information.	Restricted information to be accounted for and encrypted when passed on a discretionary basis. (e.g. laptops)
•IT Department •Cyber Security Team	Financial (PCI) (Bank Card) HIC Issued (keys,tokens)	**Restricted**	Secure platforms and controls regulating PCI.	No access to PCI information without approval and logging of date and time of access.
•Internal Auditors •External Auditors	*Various data	**Confidential & Restricted**	Check safeguards of data as approved by Board of Directors	Corporate Strategy Documents Intellectual Capital
•Personal Lines Underwriting •Commercial Lines Underwriting	Demographic (aggregate)	**Confidential**	Use paid or shared demographic information to establish line pricing	No collection or unauthorized sharing of demographic information
•Finance & Accounting •Human Resources •Legal •Marketing	HIC Corporate	**Confidential**	HR personnel info, market research, competitor analysis, development plans, financial forecasts, transaction planning.	No collection or unauthorized sharing of HIC information

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental I: Views of Data Classification

Micro View: Data Classification		
TYPE OF DATA	INFORMATION CATEGORY	CLASSIFICATION
Telephone Number	Contact	Confidential
Education	Demographic	Confidential
Weight	Demographic	Confidential
Customer Income	Financial	Confidential
Age	Demographic	Confidential
Truncated SSN	Identification	Confidential
HIC Internal Documents	HIC Corporate	Confidential
Bank Account Number (PCI)	Financial (Acct)	Restricted
Login Credentials / Tokens	HIC Issued	Restricted
License Plate Number	Government Issued	Restricted
Driver's License	Government Issued ID	Restricted
Passport Number	Government Issued ID	Restricted
Tribunal ID	Government Issued ID	Restricted
Social Security Number (SSN)	Government Issued ID	Restricted
PHI e.g. Medical Test Results	Medical	Restricted
Data of Birth	Personal	Restricted
European Customer	Personal (GDPR)	Restricted
(Nolan & Wilson, 2015)		

Macro View: Data Classification				
#	Data Category	Data -Subcategory	Classification	Authority
1	Consumer Data	Contact Info (e.g. phone, email)	Confidential	Gramm-Leach-Bliley Act (GLBA) HIPAA State Statutes & NAIC GDPR PCI DSS SOX
		Demographic		
		Financial (Income)		
		Identification (Trunc SSN)		
		HIC Corporate		
		HIC Issued	Restricted	
		Government Issued		
		Government Issued ID		
		PHI		
		Financial (PCI) (Bank Card)		
		Personal (DOB)		
		Personal (GDPR)		
2	Business Partner Data	Joint Projects	Confidential	HIC
		Technical Data		
		Use of Network		
3	Strategy Documents	Market Research	Confidential	HIC
		Competitor Analysis		HIC
		Business Development Plans		
		Financial Forecasts		
		Future Transaction Planning		
4	Intellectual Property	Business Process	Confidential	HIC
		Customer Discovery & Retention		
		New Services & Cost		
5	Emails & Messaging	Performance Reviews	Confidential & Restricted	HIPAA HIC
		Business related information		
		Personal Emails & Messages		
Data Category column by (Mahler, 2017)				

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

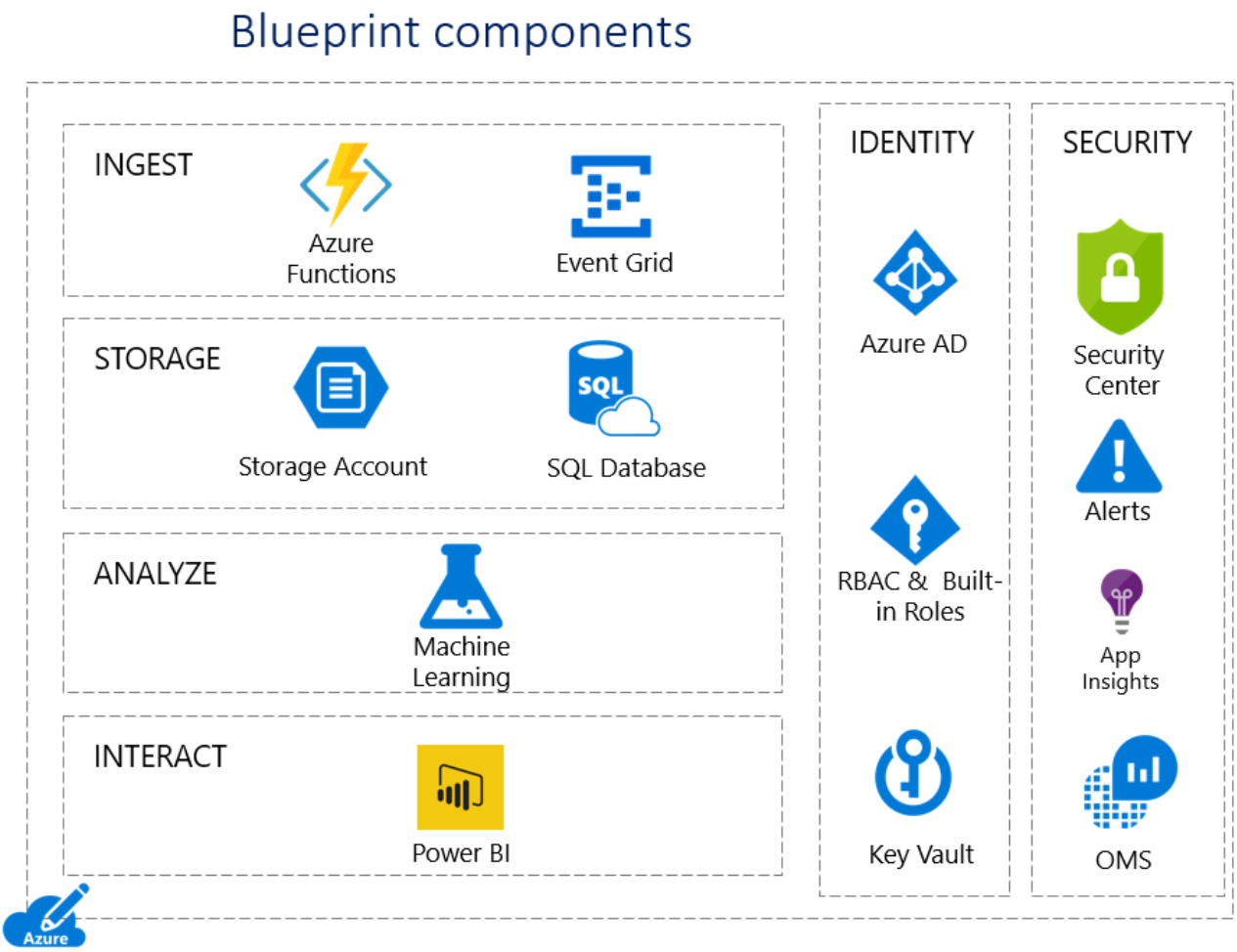
Supplemental II: HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

FUNCTION	CATEGORY	SUBCATEGORY	RELEVANT CONTROL MAPPINGS
Identify (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A),164.310(a)(2)(ii), 164.310(d)
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A),164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(A), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 16 4.316(b)(2)
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third -party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b)(1), 164.314

(HHS.Gov, 2016)

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental III: Azure Blue Prints for HIPAA Regulated Organization



CATEGORY	COMPONENT
INGEST	Azure Functions
	Event Grid
STORAGE	Storage Account
	SQL Database
ANALYZE	Machine Learning
INTERACT	Power BI
IDENTITY	Azure AD
	RBAC & Built-in Roles
	Key Vault
SECURITY	Security Center
	Alerts
	App Insights
	OMS
(Microsoft, n.d.)	

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental IV: Domains from Azure Blueprints for HIPAA Regulated Organization

#	ARCHITECTURE DOMAINS		
1	Information Protection Program	11	Access Control
2	Endpoint Protection	12	Audit Logging & Monitoring
3	Portable Media Security	13	Education, Training, and Awareness
4	Mobile Device Security	14	Third Party Assurance
5	Wireless Security	15	Incident Management
6	Configuration Management	16	Business Continuity & Disaster Planning
7	Vulnerability Management	17	Risk Management
8	Network Protection	18	Physical & Environment Security
9	Transmission Protection	19	Data Protection & Privacy
10	Password Management	(Microsoft, n.d.)	

Azure Blueprints		
Domain	**HITRUST Control**	**HITRUST CSF Requirement Statement**
3 Portable Media Security	Management of Removable Media	The organization, based on the data classification level, registers media (including laptops) prior to use, places reasonable restrictions on how such media be used, and provides an appropriate level of physical and logical protection (including encryption) for media containing covered information until properly destroyed or sanitized.
3 Portable Media Security	Information Handling Procedures	Media is labeled, encrypted, and handled according to its classification.
4 Mobile Device Security	Teleworking	The organization provides a definition of the work permitted, standard operating hours, classification of information that may be held/stored, and the internal systems and services that the teleworker is authorized to access; suitable equipment and storage furniture for the teleworking activities expressly designated for business use by authorized employees; where the use of privately owned equipment not under the control of the organization is forbidden; suitable communications equipment, including methods for securing remote access; rules and guidance on family and visitor access to equipment and information; hardware and software support and maintenance; procedures for back-up and business continuity; a means for teleworkers to communicate with information security personnel in case of security incidents or problems; and audit and security monitoring.
7 Vulnerability Management	Inventory of Assets	The inventory of all authorized assets includes the owner of the information asset, categorizes the information asset according to criticality and information classification, and identifies protection requirements commensurate with the asset's categorization.
8 Network Protection	Segregation in Networks	The organizations network is logically and physically segmented with a defined security perimeter and a graduated set of controls, including subnetworks for publicly accessible system components that are logically separated from the internal network, based on organizational requirements; and traffic is controlled based on functionality required and classification of the data/systems based on a risk assessment and their respective security requirements.
11 Access Control	Access Control Policy	Access controls are consistently managed for all systems and applications in networked and distributed environments based on the classification of and risks to the information stored, processed, or transmitted.
17 Risk Management	Risk Management Program Development	Personal identifying information (PII) is defined appropriately.
(Microsoft, n.d.)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental V: Specific Restricted and Confidential Asset Descriptions

Restricted Information		
#	**TYPE**	**DESCRIPTION**
1	Authentication Verifier	An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to: Passwords Shared secrets Cryptographic private key (CMU, 2015)
2	Covered Financial Information	"Covered information" means nonpublic personal information about a customer or other third party who has a continuing relationship with HIC. Nonpublic personal information includes customer's names, addresses and social security numbers as well as customer's ' and dependent's financial information. Covered information does not include records obtained in connection with single or isolated financial transactions such as ATM transactions or credit card purchases (CMU, 2015)
3	Electronic Protected Health Information ("EPHI")	EPHI is defined as any Protected Health Information ("PHI") that is stored in or transmitted by electronic media. For the purpose of this definition, electronic media includes: Electronic storage media includes computer hard drives and any removable and/or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, an extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks and the physical movement of removable and/or transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exists in electronic form before the transmission. (CMU, 2015)
4	Protected Health Information ("PHI")	PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component, as defined in HIC HIPAA Policy. PHI is considered individually identifiable if it contains one or more of the following identifiers: Name Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code) All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89) Telephone numbers Fax numbers Electronic mail addresses Social security numbers Medical record numbers Health plan beneficiary numbers Account numbers Certificate/license numbers Vehicle identifiers and serial numbers, including license plate number Device identifiers and serial numbers

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

		Universal Resource Locators (URLs) Internet protocol (IP) addresses Biometric identifiers, including finger and voice prints Full face photographic images and any comparable images Any other unique identifying number, characteristic or code that could identify an individual Per HIC's HIPAA Policy, PHI does not include education records or treatment records covered by the Family Educational Rights and Privacy Act or employment records held by HIC in its role as an employer. (CMU, 2015)
5	Personally Identifiable Information ("PII")	For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements: Social security number State-issued driver's license number State-issued identification card number Financial account number in combination with a security code, access code or password that would permit access to the account Medical and/or health insurance information (CMU, 2015)
6	Personally Identifiable Education Records	Personally Identifiable Education Records are defined as any Education Records that contain one or more of the following personal identifiers: Name of the student Name of the student's parent(s) or other family member(s) Social security number Student number A list of personal characteristics that would make the student's identity easily traceable Any other information or identifier that would make the student's identity easily traceable (CMU, 2015)
7	Payment Card Information	Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements: Cardholder name Service code Expiration date CVC2, CVV2 or CID value PIN or PIN block Contents of a credit card's magnetic stripe Payment Card Information is also governed by HIC's PCI DSS Policy and Guidelines (login required). (CMU, 2015)
(CMU, 2015)		

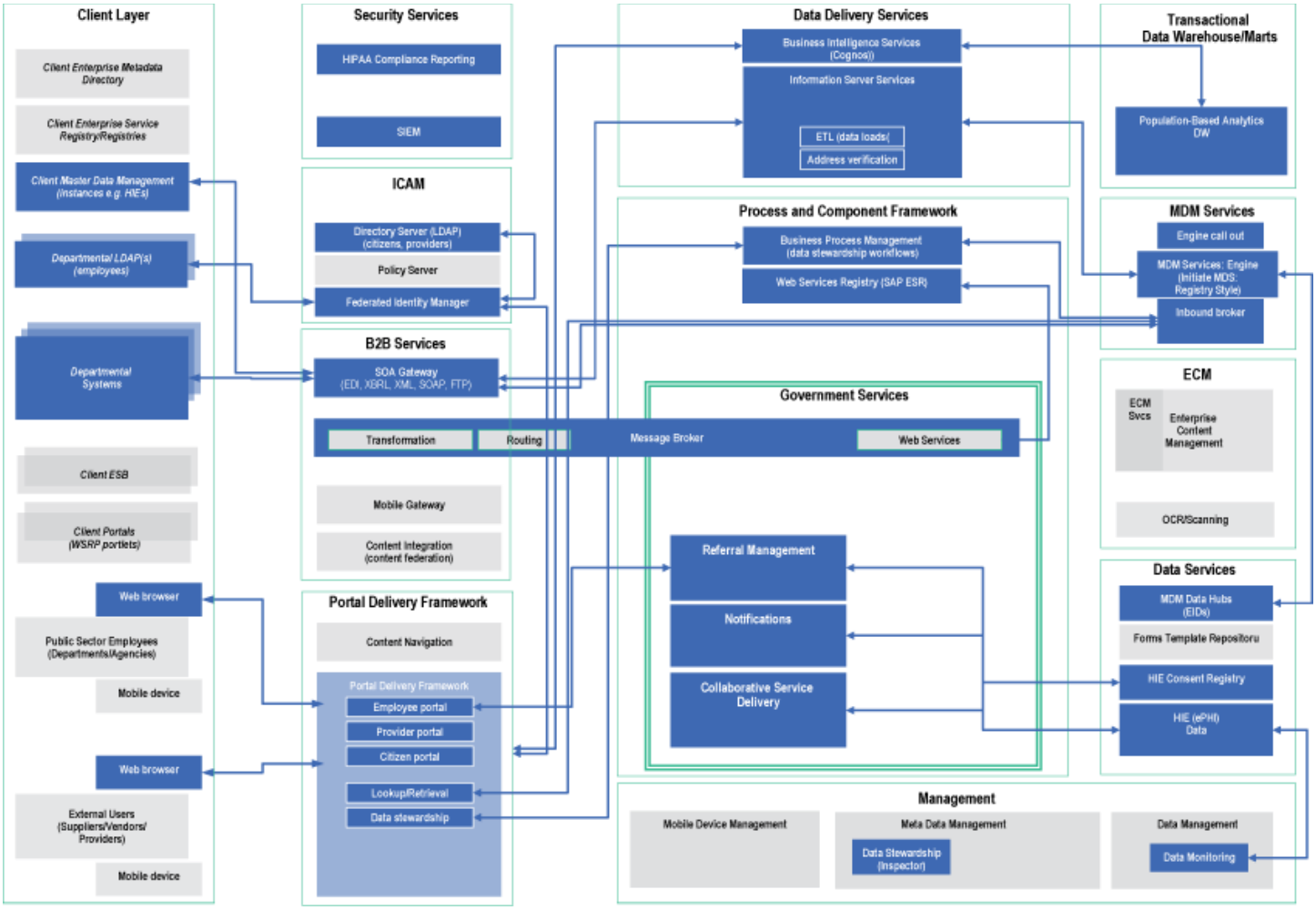
From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental VI: User Types

USER CATEGORY	USER TYPE	DESCRIPTION
Human	Employees	*Salaried or hourly staff members of the organization.*
	Systems Administrators	*Employees who work in the IT department to provide technical support to the systems.*
	Security Personnel	*Individuals responsible for designing and implementing a security program within an organization.*
	Contractors	*Temporary workers who can be assigned to any role; contractors are directly managed by the company in the same manner as employees.*
	Vendors	*Outside companies, or individuals working for such companies, hired to provide ongoing services to the organization, such as building cleaning.*
	Guests & General Public	*A class or group of users who access a specific set of applications.*
	Control Partners	*Individuals who evaluate controls for design and effectiveness.*
Non-human	System Accounts	*Non-human accounts used by a system to support automated service.*
	Contingent IDs	*Non-human accounts until they are assigned to individuals who use them to recover a system in the event of a major outage.*
(Johnson, 2015)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental VII: Technical Categories of Data Processing in a HIPAA Org through IT Architecture



(IBM, n.d.)

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental VIII: Social Media, Technology, and Purchase Behavior Data

SOCIAL MEDIA & TECHNOLOGY DATA		PURCHASE BEHAVIOR DATA	
Electronics Purchases		Amount Spend on Goods	
Friend Connections		Buying Activity	
Internet Connection Type		Method of Payment	
Internet Provider		Number of Orders	
Level of Usage		Buying Channel Preference	E.g. Internet, In Person
Heavy Facebook User		Types of Purchases	
Heavy Twitter User		Military Memorabilia/Weaponry	
Twitter User with 250+ Friends		Shooting Games	
Is a member of over 5 Social Networks		Guns & Ammunition	
Online influence		Christian Religious Products	
Operating system		Jewish Holidays/Judaica Gifts	
Software Purchases		Kwanzaa/African-Americana Gifts	
Type of Media Posted		Type of Entertainment Purchased	
Uploaded Pictures		Type of Food Purchased	
Use of Long Distance Calling Services		Average Data Between Orders	
Presence of Computer Owner		Last Online Order Date	
Use of Mobile Devices		Last Offline Order Date	
Social Media & Internet Accounts:		Online Order $500-$999 Range	
Digg		Offline orders $1000+ Range	
Facebook		Number of Orders- low-scale catalogs	
Flickr		Number of Orders- High-scale catalogs	
Flixster		Retail purchases – most frequent	
Friendster		Mail order responder- insurance	
Hi5		Mailability Score	
Hotmail		Dollars – Apparel – Woman's Plus Sizes	
LinkedIn		Number of Orders- Men's Big & Tall	
Live Journal		Books – Mind & Body/Self-Help	
MySpace		Internet Shopper	
Twitter		Highlight and color this block	
Amazon			
Bebo			
CafeMom			
DailyMotion			
Match			
myYearbook			
NBA.com			
Pandora			
Photobucket			
WordPress			
Yahoo			
ToastedDolphin			
(Nolan & Wilson, 2015)			

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

Supplemental IX: Platform Technical Links

Document	Description	LINK
Azure Blueprint NIST SP 800-53 Implementation Guide Published October 2017	This guide is designed to help cloud solution architects and security personnel understand how Azure Government services and features can be deployed to implement a subset of customer-responsibility FedRAMP and DoD security controls.	Link
Azure Security and Compliance Blueprint - HITRUST Health Data and AI Review.pdf Updated March 4, 2018	This whitepaper constitutes a review of the Blueprint architecture and functionality with respect to HITRUST-compliant customer environments, examining how specifically it can satisfy these requirements. The whitepaper also considers the interplay of Azure and customer-oriented responsibilities for Blueprint deployment, configuration, and management in a manner consistent with HITRUST. Last, the whitepaper presents an illustrative deployment use case to help the reader visualize the Blueprint architecture in action.	Link
Azure Security and Compliance Blueprint – HIPAA/HITRUST Health Data and AI Threat Model Updated March 3, 2018	This data flow diagram and threat model for the Health Data and AI Threat Model solution provides a detailed explanation of the solution boundaries and connections.	Link
Azure Security and Compliance Blueprint - HITRUST Customer Responsibility Matrix (CRM) v9.0d.xlsx Updated March 3, 2018	This workbook lists the security controls required for HIPAA and HITRUST-compliant environments and denotes how the Health Data and AI Customer solution aligns with the control requirements.	Link
(Microsoft, n.d.)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 16, 2018
Subject: Health Insurance Company (HIC) Information Identification & Classification Policy

References

CMU. (2003, May). *Information Security Program Outline.* CMU.edu. Retrieved from https://www.cmu.edu/policies/information-technology/gramm-leach-bliley-act.html

CMU. (2015, May 4). *Guidelines for Data Classification*. Cmu.edu. Retrieved from https://www.cmu.edu/iso/governance/guidelines/data-classification.html

HHS.Gov. (n.d.). Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. HHS.gov. Retrieved April 16, 2018 from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf/

HHS.Gov. (2016, February 22). *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework.* Retrieved from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf/

ISOO. (2009). *The President Executive Order 13526*. Retrieved from https://www.archives.gov/isoo/policy-documents/cnsi-eo.html#six

Johnson, R. (2015). *Security Policies and Implementation Issues, Second Edition.* Burlington, Massachusetts: Jones & Bartlett Learning

Mahler, L.D. (2017, October 26). *Beyond credit card numbers: How different types of data can impact your reputation.* Csoonline.com. Retrieved from https://www.csoonline.com/article/3235105/data-breach/beyond-credit-card-numbers-how-different-types-of-data-can-impact-your-reputation.html

Microsoft. (n.d). *Azure Security and Compliance HIPAA/HITRUST Blueprint.* Retrieved from https://servicetrust.microsoft.com/ViewPage/HIPAABlueprint

Nass, S.J., Levit, L.A., Gostin, L.O. (2009). *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research.* Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK9579/

Nolan, C., Wilson, A. (2015, October 23). *DAMA Webinar: The Data Governance of Personal (PII) Data* [SlideShare Slides]. Retrieved from https://www.slideshare.net/Dataversity/dama-webinar-the-data-governance-of-personal-pii-data

Logo from:

MarksMan Healthcare Communications. (n.d.). *HEOR – INDIA CONCLAVE (HIC).* Bna.com. Retrieved March 14, 2018 from https://marksmanhealthcare.com/heor-india-conclave/