Toolkit for Developing an Identity and Access Management (IAM) Program

Mission/Purpose
The **Identity and Access Management Program Project Team** is focused on creating a roadmap for institutions to use in developing an IAM program (or to address gaps in their current offerings).

Goals
- Provide structure or guidance for those starting IAM.
- Identify a policy framework that institutions may need to consider.
- Develop a policy template (or set of policy templates) that other campuses can use.
- Provide guidance or awareness about IAM governance.
- Identify existing IAM policies or programs and provide use cases.
- Otherwise strengthen the business side of the IAM program.

Target Audience
- Those responsible for IAM policy development.
- Those who have IAM policies in place that need to be updated.
- People or functions impacted by regulatory requirements regarding access control (e.g., GLBA, HIPAA).
- Institutions developing an IAM program or set of policies for the first time.
1. Introduction

The IAM Program—The Big Picture

As data, access, and networks continue to expand, institutions have an ever-increasing need to manage identities and access. The optimum solution for this function is a well-planned and institution-wide identity and access management (IAM) system. Identity and access management is a broad administrative function that identifies individuals in a system, and controls and facilitates their access to resources within that system by associating user rights and restrictions with the established identity. In its simplest form, IAM ensures that only the right people can access the right services at the right time.

However, within a complex organization, establishing an IAM program is not an easy task. Many stakeholders, technology areas, policies, and processes must work together for a scalable and robust IAM system. In addition, governance plays a key role in the success of any IAM program and implementation.

The Toolkit for Developing an Identity and Access Management (IAM) Program has been created as a roadmap for institutions to use in developing an IAM program (or to address gaps in their current offerings) including:

- Providing a structure or guidance for those starting IAM
- Identifying a policy framework that institutions may need to consider
- Developing a policy template (or set of policy templates) that other campuses can use
- Providing guidance or awareness about IAM governance
- Identifying existing IAM policies or programs and providing use cases
- Otherwise strengthening the business side of the IAM program

Figure 1, created by Lynn McRae at Stanford University and Internet2, illustrates the "big picture" of an IAM infrastructure—a very elegant representation of the outcome of a well-executed IAM program. It lays out all the basic elements and how they interact with each other. The left side in green represents the foundational identity management function, while the pink area on the right adds the access piece to IAM, supported by role, group, and privilege management and clearly communicated policy and governance.
Most information security practitioners already know that there is no one-size-fits-all approach to IAM but that the approach used is informed by the characteristics, culture, and capabilities of the institution. What works for one institution may not necessarily work for another. So, if the graph above is a "desired state," how does an institution get from its current state to that desired state?

What Is In Scope?
The intent of the Toolkit for Developing an Identity and Access Management (IAM) Program is to assist institutions starting a program come up with actionable steps, tasks, and the mix of foundation, policy, and technology that will work for them. Figure 2 illustrates a proposed roadmap to get from current to desired state.
What Is Not in Scope

Also most information security practitioners are already familiar with the technology aspects of IAM. For that reason, technical implementation of IAM controls and procedures (this includes evaluation, discussion, and recommendations about tools and technologies) is not included in the scope of the Toolkit for Developing an Identity and Access Management (IAM) Program. For more technical resources, please visit the IAM Tools and Effective Practices Project Team’s wiki, the Internet2 Middleware Initiative website, and the InCommon Federation website.

Assumptions

- The organization is complex enough that simple traditional access and authorization to information assets is not scalable. For example, manually managing role-based access to a student information system via LDAP groups for more than 3,000 users leads to inefficiency, user-impacting mistakes, and potential leakage of confidential data due to provisioning too much access.
- A regulatory pressure, such as the Gramm-Leach-Blileya Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA), is pressuring the organization to better manage its access control and authorization. Said regulatory pressures require that organizations have policies in place to manage access control and to produce evidence that they provide only "limited access" on a “need to know” basis. For example, within the HIPAA Security
Rule, covered entities are not only required to limit access to ePHI (electronic protected health information) but also to maintain audit logs of such access by any individual over specific periods of time.

- Certain policies, organizations, etc., are in place to support an IAM program.

2. What Comprises an IAM Program?
At a high level, an IAM program comprises three essential components:

- **A Resource and Governance Foundation**: Certain resources and conditions are prerequisites if an institution of higher education is to have a viable and sustainable program.
  - Clear and widely communicated program scope
  - Executive support
  - Implementation and operating (i.e., ongoing) budget
  - Staff, skills, and expertise
  - Governance

- **A Policy Body**: The various policies, standards, and procedures that will support the program and make it enforceable. These policies should include and take in consideration:
  - Institutional and regulatory drivers
  - Stakeholder requirements
  - Identity proofing and a credential life-cycle management process
  - Roles and responsibilities
  - Awareness and training
  - Compliance verification processes

- **Technology**: The various technology standards, protocols, infrastructure, applications, interfaces, etc., that make the implementation and automation of the program possible.
  - IAM Standards
  - Provisioning, access control, and deprovisioning tools
  - Registries
  - Authentication methods
  - Supporting infrastructure and source systems, etc.

The Toolkit for Developing an Identity and Access Management (IAM) Program focuses mostly on the foundation and policy areas of the program. As mentioned above, there are already a number of resources and groups that cover the technology aspects in great detail.

An IAM program is not a replacement or stand-in for a Social Security number (SSN) or protected health information (PHI) protection program or for a data governance or master data management program.
Resources

- Internet2 IAM Tools and Effective Practices. Numerous resources, including webinar archives, fact sheets, solution papers and publications on all facets identity and access programs.
- EDUCAUSE Identity and Access Management. Overview, publications, presentations, podcasts, and blogs regarding the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources.

3. Starting an IAM Program

There are four high-level topics to consider when implementing an IAM program, either starting from scratch or updating an existing one. These topics are:

- Program Scope
- The Institution's Organizational Landscape
- The Identification of Stakeholders
- Program Governance

3.1. Program Scope

Institutions of higher education create, collect, maintain, and make available large amounts of information in support of their educational, health care, and research missions. This information is an institutional asset that must be administered and protected in accordance with its value and in conformance with federal, state, and institutional rules and regulations. It is important to understand where the institution is starting from, and what is it trying to accomplish. A clearly stated and communicated program scope provides the following advantages:

- Frames the objectives of the program.
- Establishes the program's boundaries for the purpose of funding and time and effort required for implementation and subsequent operation.
- Helps make the case for an IAM program to executive officers.
- Saves times and energy. Policy work is not only slow—in most cases it is the bulk of the work as well, especially if you're starting from scratch. A clear scope will help reduce the number of policies required and the time needed to approve them.

The scope of an IAM program can be as broad as facilitating inter-institutional collaboration, for example, or as narrow as obtaining InCommon Assurance Silver Certification. The program scope should provide executive officers a narrative of the business case being addressed and the expected benefits. Some examples:

- Ensures that individuals have a single identity as they move through various roles in and relationships with the institution. The institution currently has at least “X” different and sometimes conflicting sources of identity information.
- Increases assurance, where appropriate, that individuals with access to data, services, and selected physical locations of the institution are who they say they are. Inconsistent, and in many cases weak, methods are used across the institution for confirming identities.
- Enables the institution to tightly align its identity assurance standards with federal and higher education standards so that individuals vetted through the identity-proofing process are
allowed access to resources at other institutions, government agencies, and other entities requiring these standards.

- Helps ensure that all access privileges granted to individuals are removed when they are no longer needed. Because access privileges are not centrally managed today, there is no automated means of ensuring all unnecessary privileges are revoked in a timely manner.
- Enhances overall security, as well as the experience of individuals seeking access privileges, by eliminating duplicative identity and access privilege data collection and storage processes throughout the institution. Today, for example, there is no single place where individuals can go to correct their identifying information and have those corrections applied in all systems.

**Key Questions to Ask**

- Does my institution have one, several, or many sources of identity?
- What sources of identity exist within the institution and what sources are authoritative for the identity population? Some examples of sources of identity include HR systems, student information systems, alumni systems, guest systems, and contractor systems.
  - The institution may need to determine what identity provisioning process will serve as the master source for all identity information. If multiple sources are needed, then a Master Data Management System should be considered to reduce the amount of complexity associated with identity, standardize the information into a common format, and eliminate incorrect data.
- Is there a regulatory pressure (federal, state, local, or industry) that is driving the need to govern identities in a mature manner? An example case could be regulations such as FERPA or HIPAA requiring "minimum-need-to-know" access to enterprise systems.
- Is there an institutional strategy or initiative that needs support?
- Are we trying to mature an existing IAM program, or mature the mechanisms by which we currently manage identities?
- Where are we, as an institution, starting from?
- What are we trying to accomplish?
- How would the IAM program align with the institution's strategic objectives?
- How important are flexibility, convenience, and ease of use?
- How difficult would application integration be with new or legacy infrastructure?
- How important is federation? Build our own or join InCommon?

**Case Studies**

- [Columbia University IAM Case Study](#)—IAM Current State section
- [Virginia Tech InCommon Assurance Implementation](#)
- [Coppin State University Identity Management Evolution](#)

**Resources**

- [Identity Management in Higher Education 2011 Report](#), EDUCAUSE Center for Applied Research
3.2. The Institution's Organizational Landscape

Scope is also informed by the institutional organizational landscape. As with everything else, the level of complexity is directly related to the number of moving pieces. Implementation of an IAM program can be relatively simple in a single institution with centralized information technology, a homogeneous organizational environment, and consistent policies compared to a similar implementation in a multi-institution university system with very decentralized IT deployment, heterogeneous environments, inconsistent policy governance, and differences in institution size, budget, and priorities. A very common mistake is to underestimate the importance of understanding institutional culture and politics in the success of any project that requires the buy-in and participation of multiple stakeholders.

Also, institutions of higher education have a broad constituency with varying degrees of affiliation. Still, all constituents have one thing in common—all require access to some type of institutional information for a determined period of time—they all become users.

At a high level, institutions can divide users into three groups based on their type of affiliation to the institution:

- **Formal affiliation**: Users whose affiliation to the institution is established by some kind of contract or enrollment. Users in this group include staff members, employee, faculty, researchers, and students.
- **Casual affiliation**: Users whose affiliation to the institution is transitory, periodic, mostly informational, and not established by a contract or enrollment. Users in this group include guests, retirees, donors, parents, library patrons, and alumni.
- **Dependent and exclusive affiliations**: Many times an individual will have an affiliation only as long as they have another, more foundational affiliation. Examples:
  - A student government official must also be a student
  - A department chair must be a member of the faculty

In some cases, affiliations are exclusive and cannot be held by the same individual at the same time. Examples:

- Accounts payable and general ledger
- Internal audit and information security
- Developer and quality assurance

Furthermore, a considerable number of users have multiple affiliations depending on the number of "hats" an individual wears while affiliated to an institution. Examples:

- Administrators with faculty appointments
- Student staff
- Staff or faculty and parent of applicant or student
- Staff and alumni
- Staff and employees who are also students pursuing a degree
- Emeriti faculty
Lastly, it is important to understand the affiliation life cycles and user transitions that should inform an institution’s user access management process. Examples:

- Student → student/worker → employee/staff/faculty → retiree
- Student → alumni/donor
- Applicant → employee/staff/faculty → former employee
- Prospective/expected user → active user → deactivated user → deleted user

The examples above are one dimensional and serial. As stated above, many times these can be multidimensional and cyclical.

**Key Questions to Ask**

- What is the organizational makeup of my institution? Single campus? University system?
- What are my institutional/departmental environments? Homogeneous or diverse environments?
- Does my institution have consistent governance policies?
- Are there significant differences in campus size, budgets, missions, and priorities?
- Are there significant differences in culture?
- Does my institution consist of fairly independent (i.e., stovepipes) or collaborative entities?
- Does my institution have and maintain multiple constituency affiliations?
- What are the existing affiliation life cycles? Are these documented? Are affiliation life cycles by role, by employment status, or both?
- What are the reasons why a c-level executive should "care" about single identity? Regulatory pressures? Data/security exposure?

**Resources**

- Access Management Use Cases Organized by Area of Interest, EDUCAUSE and Internet2 CAMP (Campus Architecture and Middleware Planning)

### 3.3. The Identification of Stakeholders

There are various ways to identify and categorize the stakeholders of an IAM program. One perspective divides them into Service Consumers, Service Providers, and Role Providers.

- **Service Consumers**: Institutional staff, faculty, students, retirees, alumni, prospective students, and members of the community access and utilize different types of information stored on and accessible via institutional systems. They use this access to perform the numerous tasks required by their respective roles or seek information about programs and services provided by the institution. Examples include:

  - Students
  - Learning resources (course management systems, library, etc.)
    - Online student systems
  - Staff
    - Employee directory
- Online human resources systems (timesheets, payroll, benefits, etc.)
- Faculty and researchers
  - Online course materials and library resources
  - Federal research agencies, funding, and data resources
- Alumni and donors
  - E-mail for life
  - Alumni directories and services
- All
  - Student/employee directory
  - Emergency notification systems
- Guests
  - Long-term with sensitive access
    - Multicenter research collaborators
    - Outsourced providers (help desk, payroll processing, food services, billing processing)
  - Long-term—may provide institution-sensitive data
    - Patients (e.g., to patient portals)
    - Research subjects (gave consent)
  - Long-term low risk
    - Visiting scholars
    - Alumni/donors
  - Short-term low risk
    - Conferences, camps, summer activities, etc.
- **Service Providers:** Entities that determine, approve, and assign the level of access to institutional systems and data based on the responsibilities, job functions, reporting, or outreach requirements based on the confidentiality of the data and subject to the restrictions imposed by federal, state, and institutional rules and regulations.
- **Role Providers:** Entities that determine, approve, and assign the procedural rules for determining the individuals' roles.
Another perspective increasingly being used in IAM identifies and categorizes stakeholders based on their respective roles in the authentication transaction that will determine the access to an information resource.¹

- **Subject** (aka user, principal, or customer)
  - The person (entity or device) that is identified
  - The subject of assertions/claims about his/her identity

- **Identity Provider** (aka credential service provider, CA)
  - Responsible for **identity proofing** of subject and issuing a **credential**
  - Producer of assertions/claims about a subject’s identity to a relying party via a credential

- **Relying Party** (aka service provider, vendor)
  - Consumer of identity assertions/claims
  - Relies on assertion to make authorization decision

Regardless of the perspective used to identify stakeholders, it is important to include others who provide ancillary and support services as stakeholders and hopefully willing participants in the implementation of the project.

- Data owners determine, approve, and assign the level of access to institutional systems and data based on the responsibilities, job functions, reporting, or outreach requirements based on the confidentiality of the data and to the restrictions imposed by federal, state, and institutional rules and regulations
- IT management (centralized and decentralized as may be the case)
- Data and policy owners—especially those impacted by the scope of the IAM implementation identified by the institution

**Key Questions to Ask**
- Authorization can be quite a challenge. How do we identify subsets of individuals/stakeholders?
- How do we keeping all stakeholders motivated and involved?

**3.4. Program Governance**
It is not uncommon in institutions of higher education to find that IAM-related tasks are scattered among various administrative functions but no one organizational area owns the program and is responsible for its operation, maintenance, and sustainability.

There are three high-level topics to consider regarding program governance:

- Program Ownership

---

• Program Funding
• Staffing: Skills, Roles, and Responsibilities

3.4.1. Program Ownership
For a program to be effective and successful, there needs to be a clear vision and strategy properly scoped and clearly communicated, as well as coordinated implementation, oversight, sustained operation, and collection of metrics to ensure that intent and objectives are being accomplished. For this to happen, accountability for the program needs to rest on an organizational unit.

Furthermore, in most cases, ownership of IAM falls along the lines of ownership of the technology used to support the function, which is why it is not uncommon to see IAM as part of the IT area. In other cases, IAM is found as part of information security (which itself is often part of IT). And one thing is clear—there is no one-size-fits-all solution—and what works for one institution may not work for another. As mentioned above, each institution will need to determine the organizational structure that best fits its organizational landscape. Some institutions leverage established steering committees, while others with distributive environments will create a separate IAM Steering Committee to establish and enforce policy and prioritize projects.

Key Questions to Ask
• How distributed is institutional data and how pervasive is its access?
• Is a formal data governance structure needed? Is there one in place already?
• Where should IAM reside? IT operations? Information security? Other?
• How is the identity vetting and credentialing of staff, faculty, and students performed? By whom?
• Centralized or decentralized person registry?
• What are the sources of authority for staff, faculty, and student identities? Where do these systems reside?
• How do application and data owners determine and approve access or their applications? Who is the appropriate business owner that ultimately should be granting access to said applications?

Case Studies
• Columbia University IAM Case Study—see the IAM Policy and Governance section

Resources
• IAM Governance wiki, developed by IAM-TEP project team
• Information Security Governance wiki

Program Funding
The way the program is funded and sustained depends on who owns and is responsible for the program and on answers to some of the key questions asked in the section above. Options include a stand-alone capital project, falling under the umbrella of a large-scale institution initiative (e.g., ERM, HR System, etc.) or long-term refresh using operational funds.
Key Questions to Ask

- How will the implementation costs be handled?
- Where will the ongoing costs be associated?
- Which department will cover the necessary staffing costs?
- What long-term funding plans are needed for upgrades and/or replacement?

3.4.2. Staffing: Roles and Responsibilities

The skill set and staffing needed to implement and support an IAM program depends on the institution’s IAM program maturity. For simplicity, this toolkit focuses on initial implementation/ramping-up efforts and ongoing operations/maintenance.

Roles

Ramping Up

- Institutional subject matter experts (SMEs)
- Human resources
- Registrar
- Chief information officer
- Chief information security officer
- Identity management SME
- Budget manager
- IT steering committee
- Internal audit
- Physical access representatives
- Data owners/stewards
- Programmers
- Database engineers
- Systems engineers
- Security engineers

Ongoing Operations

- Institutional SMEs
- Data stewards
- Account administrators (security administrator)
- IAM team (established team, or potentially other IT groups such as server team)
- CISO (for day-to-day policy enforcement)

Responsibilities

Ramping Up

Functional

- Create a required skill set inventory
- Identify roles and resource owners
- Perform policy gap analysis and create mitigation plan
- Define program requirements
• Work with institutional policy owners to define and create required policies, standards, and procedures
• Define a role provisioning workflow
• Define and communicate standards for proofing and vetting identities

Technical
• Identify all relevant identity and access stores (technical integration points)
• Define required technical infrastructure
• Define and communicate implementation strategy (buy versus build):
  
  **Buy**
  ▶ Novell
  ▶ IBM
  ▶ Oracle

  **Build**
  ▶ Signet
  ▶ Grouper

Ongoing

Functional
• Work with resource owners to establish a role-based access control (RBAC) workflow
• Work with institutional policy owners to update and maintain relevant policies, standards, and procedures

Technical
• Ongoing maintenance and support of the infrastructure
• Develop integrations as needed

**Key Questions to Ask**
• How distributed is institutional data and how pervasive is its access?
• What are the institution's IAM tools, processes, models, and documentation currently in place?
• Is a formal Data Governance structure needed? Is there one in place already?
• Where should IAM reside? IT operations? Information security? Other?
• Are IAM roles and responsibilities defined and communicated?
• Centralized or decentralized person registry?
• Where are SMEs and technical/nontechnical staff coming from?
• What should we grow, what should we buy, and what should we outsource?
• Who is responsible for supporting users and IAM applications?
• Who is responsible for auditing identity providers' practices and what standards are used?
4. Developing a Policy Framework
An effective and sustainable IAM program requires the support of many policies to improve the institution's identity and access security posture. Most institutions have a base information security policy set, which includes most of what is needed. To support an effective IAM program, institutions should consider the following:

Core Body of Policies
- Access Management Policy
  - Identity life cycle
  - Credential issuing and revoking
  - Standard schema definitions (e.g., eduPerson)
  - Business need/risk-based access
  - Role-based access control
  - Nonconsensual access by nonowners
  - Eligible affiliations
  - Attribute release policy
  - Remote access policy

Additional Policies
- Data Inventory and Classification Policy
- Federated Access Policy
  - Federation operating procedures
  - Attribute release policies
- Acceptable Use Policies

Policy Template(s) or Outline of Model Policies
Key elements that an IAM policy should include:

1. Policy statement
2. Definitions, data ownership, and accountability
3. Creation, management, and revoking of identifiers
4. Requesting and granting access to information resources
5. Types of identifiers
6. Identifying and authenticating to information resources
7. Remote identifying and authentication
8. Removing and changing access to information resources

Key Questions to Ask
- How distributed is institutional data and how pervasive is its access?
- What authoritative source(s) of information regarding the identity and attributes of individuals granted access to data, services, and physical locations should be cited in the policy?
- What IAM roles and responsibilities should be explicitly defined in the policy?
With what state, national, and/or international standards and best practices will the institution’s IAM program align? Should these be cited in the policy?

Case Studies

- Implementing True Identity Management on Your Campus and Planning for Success (and Avoiding Critical Mistakes), a presentation at the EDUCAUSE Conference 2012, for lessons learned from colleagues at Massachusetts College of Art and Design, The George Washington University, and Princeton University.

Use Cases: Existing IAM Policies or Programs

- University of Florida IdM Policy (2009)
- Wofford College IdM Policy (2009)
- Michigan Technological University IdM Policy (2011)
- Georgia Tech IdM Policy
- Cornell IdM

Resources

- Cornell IT Policy Framework
- EDUCAUSE Library Page—Identity Management Policy
- Brown University attribute release policy for web single sign-on (SSO)

5. Glossary of Terms, Acronyms, and Concepts

**AMC**: Academic Medical Center. An institution that (1) contains a medical school that trains physicians, (2) supports research activities involving laboratory sciences and/or clinical sciences, and (3) delivers health care services that may include one or more hospitals, clinics, or physician office practices. Typically these centers fall under a larger university and are considered to be the HIPAA-covered component of the university.

**CA**: Certificate Authority. An entity that issues digital certificates. These digital certificates are electronically signed by the creating certificate authority and are used to delegate trust to the provisioned certificate. Commonly, a well-known certificate authority, such as VeriSign or Thawte, is used to create digital server certificates for reputable and secure electronic transactions.

**Credential**: Evidence of entitlement to rights or privileges. For example, an access credential to a student information system is a secret key, or password, known only to the user.

**DLP**: Data Loss Prevention. Systems or applications that are developed and implemented to detect and potentially prevent inadvertent, accidental, or intentional leaks of confidential information outside authorized channels. These tools can be deployed at the endpoint (such as desktops or servers), the network perimeter, and within the enterprise network.
ECAR: EDUCAUSE Center for Applied Research. ECAR provides research and analysis about information technology in higher education for IT professionals and higher education leaders.

EHR/EMR: Electronic Health/Medical Record. An electronic record of an individual’s medical history that is maintained by health professionals and official agencies generated by one or more encounters in any care delivery setting. The EHR and EMR tend to be supported by central systems and applications to streamline clinical workflow for storage, access, and processing of patient care. It can also be used for evidence-based decision support, quality management, and outcome reporting.

FERPA: Family Education Rights and Privacy Act. A federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

GLBA: Gramm-Leach-Bliley Act. This act requires in-scope institutions to create information security standards. GLBA defines "financial institutions" as: "…organizations that offer financial products or services to individuals, like loans, financial or investment advice, or insurance."

HIPAA: Health Insurance Portability and Accountability Act. The leading health care regulation that governs the use and disclosure of protected health information (PHI). This regulation is broken up into two sections, the Privacy Rule and the Security Rule. The Privacy Rule requires that covered entities restrict the user and disclosure of PHI and implement administrative requirements to safeguard PHI. The Security Rule applies to electronic PHI (ePHI) and establishes standards to protect ePHI leveraging administrative, physical, and technical safeguards.

Identity Proofing: The process of providing sufficient information (e.g., identity history, credentials) to a service provider for the purpose of proving that a person or object is the same person or object it claims to be.

Identity Provider (IdP): The organization responsible for the processes associated with enrolling a subject and establishing and maintaining the digital identity associated with an individual or nonperson entity (NPE). These processes include identity vetting and proofing, as well as revocation, suspension, and recovery of the digital identity. The IdP is responsible for issuing a credential, the information object or device used during a transaction to provide evidence of the subject's identity; it may also provide linkage to authority, roles, rights, privileges, and other attributes.

LDAP: Lightweight Directory Access Protocol. An application protocol for accessing and maintaining distributed directory information services over IP.

Master Data Management System: Master Data Management (MDM) comprises a set of processes, governance, policies, standards, and tools that consistently defines and manages the master data (i.e., nontransactional data entities) of an organization. MDM has the objective of providing processes for collecting, aggregating, matching, consolidating, quality assuring, persisting, and distributing such data throughout an organization to ensure consistency and control in the ongoing maintenance and application use of this information.
**PHI:** Protected Health Information. Any information, whether oral or recorded, in any form or medium that (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house; (b) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and (c) identifies the individual or provides a reasonable basis to believe the information can be used to identify the individual, such as information found within the Privacy Rule health identifiers.

**Privacy Rule Health Identifiers:** Eighteen unique identifiers that, when stripped from health information, are no longer protected by the Privacy Rule. Data that has the 18 identifiers removed can be considered "de-identified" and used or disclosed without consequence, such as for research.

1. Names.
2. All geographical subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Phone numbers.
5. Fax numbers.
6. Electronic mail addresses.
7. Social Security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
15. Internet Protocol (IP) address numbers.
16. Biometric identifiers, including finger and voice prints.
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

**SIEM:** Security Information and Event Management. Systems that are designed to collect, normalize, aggregate, filter, correlate, analyze, and report on log information from several log sources into a common format in a central location in order to assist security professionals in
filtering, monitoring, and managing information security events throughout the enterprise. These tools are used for both compliance and resource monitoring as well as to discover security breaches or targeted attacks.