Beth Israel Deaconess Medical Center

BIDMC

Data Frameworks

Information Systems

Ayad Shammout
1-1-2015

Beth Israel Deaconess Medical Center

Contents

Beth Israel Deaconess Medical Center

Document Control

1. Document Approval

Name	Date	Comment

2. Document Version Control

Version	Status	Date	Prepared By	Comment
0.1	Draft	8/1/2014	Ayad Shammout	
1.0	Final	1/1/2015	Ayad Shammout	

3. Review Date

These guidelines will be reviewed in May 2016

Purpose

The purpose of this document is to ensure that all the Beth Israel Deaconess Medical Center (BIDMC) data are evaluated, properly classified and labeled and that the appropriate access controls are implemented to protect the data. These guidelines are developed to provide a consistent and structured approach to classification and labeling of sensitive information, and encourage better practices in protective security procedures to be used by all BIDMC users.

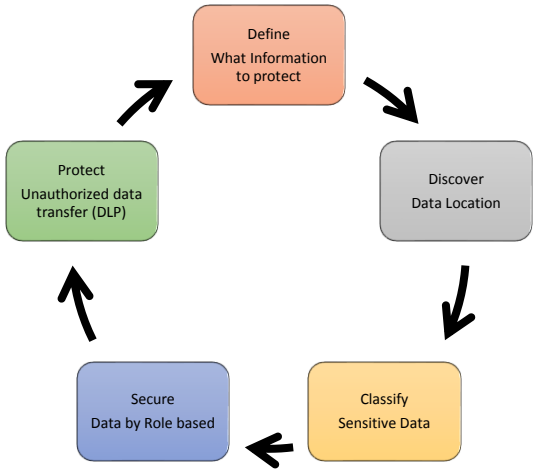
Overview

Data Frameworks is a set of policies and rules with defined approach for making BIDMC data more secure and protected.

This is a methodical approach starts with data discovery process to locate all data (structured and unstructured) and create metadata repository, followed by data categorization to identify data based on its level of sensitivity, value and how critical it is to the organization.

The Data Frameworks will provide a new data management model to provide the means to identify, locate, describe and assess how the data assets can be managed and protected.

Data Classifications Lifecycle



The Data Classifications process is a continuous cycle that starts with defining what information to protect and implement the discovery phase to find where the data is located. Next is how to secure the data where it's stored and monitor the data usage. This leads to protect the data from beaching and unauthorized access.

1. Data Discovery

A discovery process is essential to find/identify all data storage and volume (size) to help establishing a best practices and standards to control who, how and why data access is requested.

1.1. Discovery Plan

The Data discovery is a long process and will require the assistance and cooperation between many IT and business groups, technologies and resources. It will include interviews with different application/system owners to discuss data ownership and data contents, and review the methods of data discovery for each group and define challenges and access to data.

1.2. Implementation Plan

There are multiple regulations, policies, owners and procedures that dictate how data can be discovered and categorized. There are different architectures, platforms, file systems, and applications will require different methodology in order to discover and identify data contents and types. The plan is how to perform the discovery and categorize the data sets and create the metadata repository to store the data types, location, structure, system and application types.

1.3. Discovery Tools

Data Discovery assessment phase requires different tools to scan and identify data subject to Data Classifications and Policies. Data exist in different platforms and stored in multiple locations, there will be manual and automated way to utilize the database scanning, file systems and network scanning tools to handle the diversity of sources and formats of data. During the planning phase, the IT team will recommend what tools can be used and the methods to implement the data discovery.

1.3.1. Tools

There are different tools will be used to discover data in different locations (structured and unstructured) by scanning different architecture and platforms. The following is a list of possible tools that can be used during the discovery process:

i. Database Scanning
    1. DB Scripts (custom scripts)
    2. 3rd Party Tools (i.e. Data Recon)
    3. DB Native Tools (i.e. Auditing and Profiler)

ii. File Systems scanning
    1. Varonis
    2. OpenDLP
    3. Nessus Compliance Checks
    4. Spider
    5. MS Discovery and Risk Assessment Server
    6. MS Audit and Control Management Server

iii. Network scanning
    1. Nexpose

iv. Applications
    1. Manual discovery

1.3.2. Discovery Requirements

The following are required in order to run a successful data discovery:

1. Credentials: access to different data types across the environment.
2. Host-based Agents: some 3rd part tools may require an agent installation to scan the data on every host.
3. Application access: some applications data are encrypted or structured that can't be interpreted properly, direct application access is required to ensure that data is collected and documented.
4. Network scanner: searching across different operating systems (Windows, UX and Linux) to collect and locate sensitive data in agentless mode.
5. Metadata Repository: the collected data will be stored centrally in a repository for analyzing, correlating the data and integrations from different sources. The discovery team will use the data to perform a high level review and identify the sensitive data locations for the effectiveness of Data Classifications.

1.4. Summary

The data discovery phase is an essential step in gathering and collecting data across the environment utilizing different tools and working with different IT and business group. The discovery assessments provide an important information to develop a metadata repository which lead to build a solid foundation to properly develop Data Classifications.

2. Data Classifications

The purpose of data classification is to establish a framework for classifying data based on its level of sensitivity, value and how critical it is to BIDMC as specified by the Information Security Policy.

After completing the Data Discovery Assessments, the next phase will start with reviewing the data and information assets were collected in the Data Discovery Assessment phase. This task will follow with a systematic approach to classify/categorize the data according to Data Classifications Matrix in the next section 2.1.

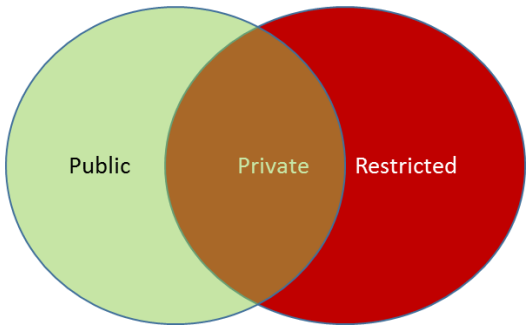
Data Classifications is an important process to enhance data protection and management and gives visibility of BIDMC data content. It is necessary to invest and apply the security policies where it is needed and protect the sensitive data with highest security measures.

2.1. Data Classifications Levels

The data classification analysis function is the process of categorizing the data according to level of sensitivity, the table below list the Personal Identifiable Information (PII) and Confidential Data identifiers and will be used in identifying what is considered as sensitive data.

Personal Identifiable Information (PII)	**Confidential Data**
Social Security Numbers	Medical Records
Credit Card Numbers	Financial Data
Name	Patient Lists
Addresses	Account Numbers
Phone Numbers	Credentials
Date of Birth	Regulatory Data

There are different Data Classifications levels:



The following table describes the security controls that will be implemented around each data classifications level.

	Data Classifications		
	Public	Private	Restricted
Definition	Data that warrants basic protection from unauthorized tampering, and can freely disseminated by anyone. Unauthorized disclosure, alteration or destruction of the data would result in little or no impact to BIDMC	Data that is not explicitly classified as Public or any of the other classifications of data should be treated as Private data. Unauthorized disclosure, alteration or destruction of the data could result in a moderate level of impact to BIDMC	Data protected by privacy regulations, confidentiality agreements or industry standards. Unauthorized disclosure, alteration or destruction of the data could cause a significant level of impact to BIDMC
Security	No security controls are required to protect the confidentiality of public data, some controls is required to prevent unauthorized modification or destruction of Public data.	A reasonable level of security controls needs to be applied to Private data.	Restricted data will warrant the highest level of security controls within the organization
Example	Affiliates information, press releases, marketing material and event information.	General employment data (excluded SSN, Bank Info, Salary, etc.)	Medical records, patient data, SSN, and credentials

It is important to understand the Data categorized according to the Data Classifications Matrix by analyzing how to measure the impact of an incident and potential violation of data access to the types of data classification (see Figure 1).

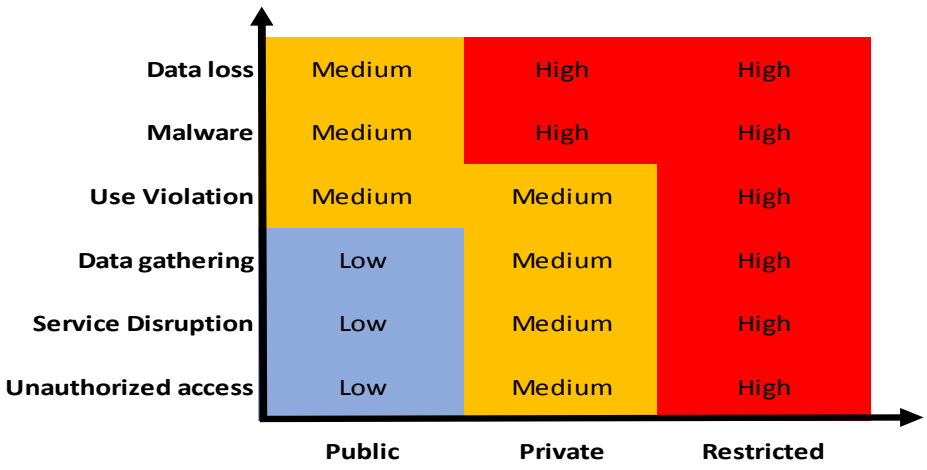


Figure 1

As the type of the events escalate the security risk will be higher, the chart in figure 1 shows the impact of an event on data classifications.

The following flow diagram describes the Data Classifications procedure, by using the flow diagram in Figure 2, it will help classify to determine the appropriate classification level for the data.

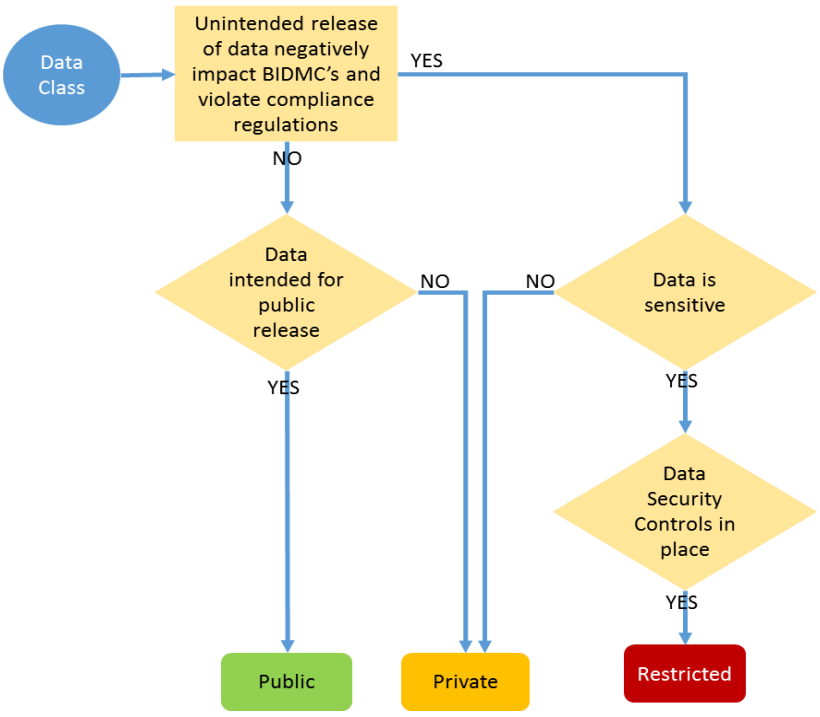


Figure 2

2.2. Data Security Controls

The Data Classifications will enforce the security controls to protect the data from loss and violation. The next matrix describes security controls that could be implemented around specific data types. The policies that address data classifications should define general security controls for the access, sharing, storage and destruction to specific data types. The higher the security control is proportional to the impact level when data is accessed; for example, if confidential data requires strict security controls, unauthorized access or disruption to that data would dictate a higher impact and quick resolution.

2.2.1. *Data Access Controls:*

	Data Classifications		
	Public	Private	Restricted
External Network Transmission (Wired and Wireless)	No special requirements	Allow Remote access only with SSL VPN	Encryption where technically feasible. Allow remote access only when critical need and with SSL VPN access
Portable Electronic Devices (Smartphones and Tablets)	No special requirements	Allow with appropriate access controls	Do not use
Websites (External and Internal)	No special requirements	Intranet/Internet sites with appropriate access controls	Only Intranet sites with restricted access controls

2.2.2. *Data Storage Controls:*

	Data Classifications		
	Public	Private	Restricted
Servers	• Strong Password • Locked in physically secure server room	• Strong Passwords • Access restricted to specific groups • Locked in physically secure server room • Annual Access Reviews	• Strong Passwords • Access restricted to specific individuals • Locked in physically secure server room • Auditing enabled • Encryption enforced • Annual Access Reviews
Workstation & Laptop	• Strong Password • Auto Lock workstation & laptop when not in use	• Strong Password • Auto Lock workstation & laptop when not in use • Only secure workstation or laptop in vehicles on short term • Do not use in public places	• Strong Password • Hard Drive Encryption • Auto Lock workstation & laptop when not in use • No workstation or laptop in vehicles • Do not use in public places

2.2.3. *Data Destruction Controls:*

	Data Classifications		
	Public	Private	Restricted
Hard Drives and Removable Media	Delete file from storage device	• Full Format storage device • Use of approved vendor for destruction	• Securely wipe or destroy storage device • Requires approval and auditing for destruction
Electronic files	Delete file	• Delete file • File delete approval	• Securely delete files • Requires approval and auditing for deletion

Classifying data defines data protection guidelines and security policies specific to sensitive data. Once the data is classified, we can properly allocate resources, develop strict security measures to protect the confidentiality and integrity of the data. The data frameworks are set of rules and controls for data discovery, storage, protection and delivery.

Summary

Data is a critical asset of the Organization, its business partners, and its patients. All individuals employed by BIDMC are responsible for protecting the confidentiality, integrity, and availability of the data generated, accessed, modified, transmitted, stored and/or used by the Organization stored in different storage devices and media. The protection of the Organization data is governed by a regulations relating to privacy and security.