Global Information Assurance Certification Paper

Unique User Identification Compliance using BindView Solutions

GIAC HIPAA Security Certificate (GHSC)
Version 1.0 (February 17, 2004)
Practical Assignment

Lou Mancel
February 10, 2005

Table of Contents

Abstract

This document discusses helping to ensure Health Insurance Portability and Accountability Act (HIPAA) compliance of U.S. Code of Federal Regulation Section §164.312(a)(1)(i) Unique User Identification using BindView solutions. The sample covered entity is a small healthcare provider that needed help with both policy creation and auditing.

The BindView software that is used in this scenario for the policy creation is BindView Policy Operations Center. “Created in conjunction with the META Security Group, Policy Operations Center provides detailed guidance and best practices templates to speed creation of a written policy that communicates the risk appetite of an organization. Once policy is created, Policy Operations Center communicates it to the organization and documents acceptance of deployed policy, providing important evidence of the organization’s security and compliance efforts.”[1]

The audit assessment tool used is bv-Control for Windows. This is one of the BindView products that allows “organizations to take a proactive, ongoing approach to protecting their multi-platform environments through in-depth reporting and analysis that assesses their risk posture from an internal and external perspective.”[2]

Assignment 1 - Environment

MHealth is a small covered entity (CE) that is a healthcare provider consisting of 250 employees that have access to the network. Networking for MHealth is a Windows 2000 Active Directory environment. All workstations are Windows XP Professional.

MHealth uses Microsoft Windows SQL databases for the storage of their electronic protected health information (EPHI). All SQL databases use Windows mode only to require the user to first authenticate to Windows. Windows authentication is monitored and is potentially more secure than the standard unmonitored SQL server model. The SQL Server database files storing the EPHI reside on the files system and also use NTFS permissions to secure who has access to those files. This helps prevent users who do not have login permissions to the EPHI to copy the database files to their own server where they have login permissions to gain access to the data.

With access to EPHI based on the login id, it is critical to insure that all personnel have unique User IDs.

Assignment 2 – Explanation

Unique User Identification

U.S. Code of Federal Regulation Section §164.312(a)(1)(i) states the following:
"A covered entity must in accordance with §164.306:

(a)(1) *Standard: Access Control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

(2) *Implementation specifications:*

(i) *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity."[3]

This required access control standard is used to assure only those persons with access rights access the EPHI. By using a unique name, every user must login using that User ID for identification and tracking.

"Identification is the process by which a subject professes and identity and accountability is initiated…Once a subject has been identified, the identity is accountable for any further actions by that subject. IT systems track activities by identities, not by the subjects themselves. A computer doesn't know one human from another, but it does know that your user account is different from all other

user accounts." [4]

MHealth uses the user account for both login and for access to the Windows SQL databases that house the EPHI. All users have individual IDs and are not to share them. This allows for accountability through log files and tracking. By using unique User ID's having a combination of numbers and characters, it makes it more difficult to guess an account's User IDs and slow down the social engineering. Valid users should have User IDs. Disabling and deleting old accounts is a necessity. Identifying contract users and temp users procedures should be followed to easily identify them through description properties which are only valid for the needed time period.

Assignment 3 - Policy

Sample Unique User Identification Policy:

The following policy is an example which could be used to help ensure compliance with U.S. Code of Federal Regulation Section §164.312(a)(1)(i) on Unique User Identification. This policy is from the BindView Policy Operations Center "Sample Access Control Standard"[5] template which I have modified and minimized to just show those areas that are valid for the example of *Unique User Identification Policy* for MHealth.

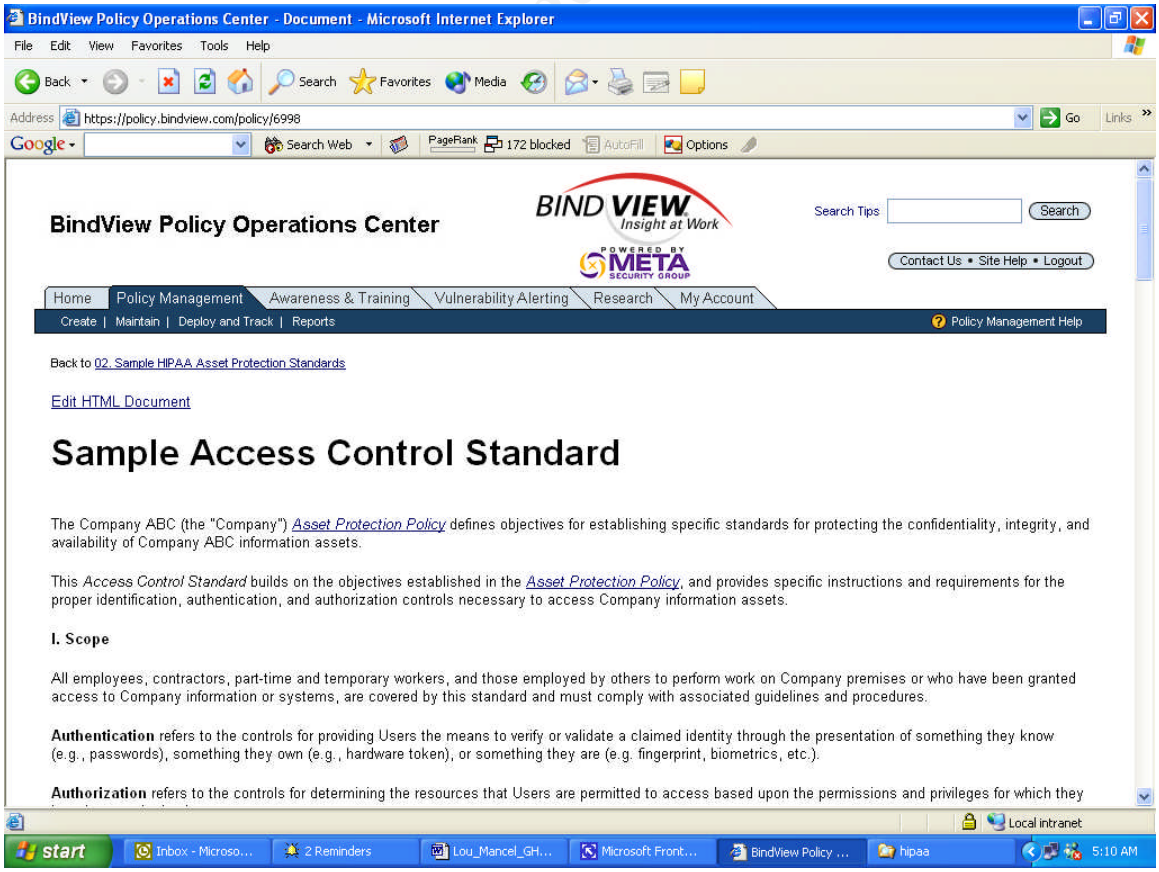

Figure 1: BindView Policy Operation Center "Sample Access Control Standard" Template [6]

This policy shows with the hyperlink and existence of the *Information Security Program Charter* that security is a corporate concern. With CEO and CIO buyoff and with the top individuals signing off, it will make it easier for policies and standards to be implemented. The *Unique User Identification Policy* references the *Asset Protection Policy, Asset Identification and Classification Policy*, and the *Information Classification Standard.* The practice of not having all policies in one document makes it easier for change control and also for the proper signature of the officer responsible for that level of policy. These are hyperlinked at MHealth for ease of readability.

This policy states the scope, the requirements to be audited against, the responsibilities, enforcement, and the signature of the Chief Information Security Officer.

Unique User Identification Policy

The MHealth "(the "Company") *Asset Protection Policy* defines objectives for establishing specific standards for protecting the confidentiality, integrity, and availability of Company information assets."[7]

This *Unique User Identification Policy* "builds on the objectives established in the *Asset Protection Policy*, and provides specific instructions and requirements for the proper unique identification controls necessary to access Company information assets.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company premises or who have been granted access to Company information or systems, are covered by this standard and must comply with associated guidelines and procedures."[8]

"**Identification** refers to the controls for providing Users the means to convey their identities through the use of pre-determined identifiers.

Information assets are defined in the *Asset Identification and Classification Policy*."[9]

"**Sensitive information** refers to information that is classified as Restricted or Confidential. Refer to the *Information Classification Standard* for confidentiality classification categories."[10]

II. Requirements

A. Unique User Identification

1. Each User must have a unique account identifier or User ID that is alpha-numeric.
2. "User login ID's should be at a minimum six characters in length."[11]
3. "User communities and working groups must not share a single User ID for system access to ensure accurate accounting of user access and actions.
4. User IDs should not be shared or used by anyone other that the User to whom they are assigned. Users shall be accountable for all activity associated with their assigned User IDs.
5. User IDs should be added, modified, and deleted in accordance with Company-approved account management processes.
6. User IDs must be disabled within twenty-four (24) hours of notification of a status change (for example, termination or change in job).
7. User IDs that are unused, dormant, or inactive for forty-five (45) days must be disabled.
8. User IDs that are disabled for ninety (90) days must be deleted.
9. Temporary User IDs (for testing, contractors and temporary employees) should have an account expiration date that coincides with the anticipated end of employment, testing, or contract."[12]

"III. Responsibilities

The Chief Information Security Officer (CISO) approves the "[13]*Unique User Identification Policy*. "The CISO also is responsible for ensuring the development, implementation, and maintenance of the"[14] *Unique User Identification Policy*.

"Company management, including senior management and department managers, is accountable for ensuring that the"[15] *Unique User Identification Policy* "is properly communicated and understood within their respective organizational units. Company management also is responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the"[16] *Unique User Identification Policy*.

"Asset Owners (Owners) are the managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CIO will make the designation. The Owner is responsible for defining processes and "procedures that are consistent with the"[17] *Unique User Identification Policy*; processing requests associated with Company-approved access request procedure; ensuring the revocation of access for those who no longer have a

business need to access information assets; and ensuring the access controls and privileges are reviewed at least annually.

Asset Custodians (Custodians) are the managers, administrators and those designated by the Owner to manage, process or store information assets. Custodians are responsible for providing a secure processing environment that protects the confidentiality, integrity, and availability of information; administering access to information assets as authorized by the Owner; and implementing procedural safeguards and cost-effective controls that are consistent with the"[18] *Unique User Identification Policy*.

"Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for familiarizing and complying with the "[19] *Unique User Identification Policy* "and associated guidelines; following Company-approved processes and procedures to request and obtain access to information assets consistent with the Owner's approved safeguards while under the User's control."[20]

"IV. Enforcement and Exception Handling

Failure to comply with the"[21] *Unique User Identification Policy* "and associated guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws."[22]

"Requests for exceptions to the"[23] *Unique User Identification Policy* "should be submitted to the"[24] Chief Information Security Officer "in accordance with the *Information Security Standards Exception Procedure*. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this standard will continue to observe the"[25] *Unique User Identification Policy*.

V. Review and Revision

The *Unique User Identification Policy* "will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature

<Insert Name>

Chief Information Security Officer"[26]

Assignment 4 – Option A - Auditing

Auditing for Unique User Identification:

Before engaging with an audit, there must be a negotiation as to what the statement of work should consist. This states what we are responsible for, the expectations of what will provided before we arrive, the areas of the environment that we are going to assist with, and the scope and timeline of what we will be assisting. It also states that we will be having an administrator or security person with us at all times. This is for both security safeguards on their part, and also for knowledge transfer to occur from us.

When I get on site, we have a kickoff meeting so that I can meet all of the people that I will be working with. Asking for the policies and procedure documentation is a crucial step so that I know what to modify on the queries to match their environment. This is generally met with one of two responses. They either have documentation and are quite familiar with it, or they look at me with the "deer in the headlight look" and expect our software to have all of the answers.

We discuss the goal of the evaluation of their environment and if there are any changes from the statement of work. Depending on their goals, this initial installation may be used for documentation for risk analysis, confirmation that their environment is secure and following policies, or preparation for the auditors by doing a vulnerability assessment.

I. Define the Rules

Policies must be in place. This includes but is not limited to the written and signed *Information Security Program Charter,* Policies, Standards, and Procedures of how they are going to handle changes. The example of what is expected with User IDs as stated in the *Unique User Identification Policy.* Without documentation, there is not a measured method to audit against. "According to 68 Federal Register at 8361, documentation "must be detailed enough to communicate the security measures taken and to facilitate periodic evaluations pursuant to section 164.308(a)(8)."[27]

II. Publish the Rules

Education on Policies is essential. Policies must be distributed out to the users so that they know about them and accept them. It is all well and fine to write the massive amount of paperwork that one must do for documentation, but if it is

kept within a room and never distributed to the users, it is worthless, and one have just wasted time writing it. Classes and continual education of the updates of policies is essential for the security to work. If users are educated as to why it is important to have a Unique User ID, not to share their User IDs, they will be more inclined to follow the policy.

III. Audit environment

Do a vulnerability assessment on the environment against what has been documented with the policies. This will involve many people including but not limited to the audit committee, security, and the administrators. With more people involved, you should get less pushback about what you are doing. I have found that once they realize you are not being the bad guy and going for their job, but instead seeing what can be improved, most people are very inclined to help.

"A review of internal systems and a comparison to current industry best practices is recommended."[28] The SANS Step by Step guides are very helpful and located at the SANS Institute Web at https://store.sans.org. The second site is The Center for Internet Security – http://www.cisecurity.org. The Center strives to reduce the frequency of failures and attacks, and the losses that arise from them. The mission of the Center "is to help organizations around the world effectively manage the organizational risks related to information security by providing them with methods and tools to improve, measure, monitor, and compare the security status of their own Internet-connected systems and appliances plus those of their business partners."[29] The CIS provides tools and methods of how to help secure the technical internet environment. They are continually updating the methods and they have known benchmarks to compare against. HIPAA security standards are technology neutral so it is up to the CE to choose the appropriate technology to protect the EPHI, so use of industry standards is of great benefit.

The following queries for assessment were created using BindView's bv-Control for Windows.[30] All fields, field descriptions, filtering and sorting names are part of the product.

A. Unique User Identification Auditing Items

1. Each User must have a unique account identifier or User ID that is alphanumeric. This audit check will be a manual process to confirm this. I have included the first and last names of the user so that the auditor can compare the User ID to them. A query can be run and reviewed and signed off by the auditor when this is done.

"bv-Control for Windows Query: Unique Account Identifier
Data Source: Users
Fields: Domain/Workgroup Name: This field returns the name of the domain or workgroup that owns the user account.

Machine Name: This field returns the name of the machine that owns the user account. “N/A” is returned if the user is a domain account.
Fully Qualified Name:
User Logon Name: This field returns the user principle name.
First Name: This field returns the first name of the reported user.
Last Name: This field returns the last name of the reported user.”[31]

2. User login ID’s should be at a minimum six characters in length. This audit check will be a manual process to confirm with the query.

This check could be combined with the “Unique Account Identifier” query to confirm that they confirm with the policy. This will be a manual check of the report.

3. User communities and working groups must not share a single User ID for system access to ensure accurate accounting of user access and actions. Check for logged in ID’s over the time that the account should be active. Manual and spot checks to confirm that users do not leave the machines logged in when not in use.

This check looks at sessions on machines that have been logged in for more than one day and also the last activity on that machine. The results could show habits of not logging out and allowing other users to use the same User ID.

“bv-Control for Windows Query: Machines that have been logged in for more than one Day
Data Source: Sessions
Fields: Domain/Workgroup Name: This field returns the name of the domain or workgroup that owns the user account.
Machine Name: This field returns the name of the machine acting as the resource server for the session.
Client Machine Name: This field returns the machine name of the client computer.
User Name: This field returns the name of the user or special account that is logged on for the session.
Time since Start of Session: This field returns the time the session has been open.
Time Since Last Activity: This field returns the amount of time that has elapsed since there was any activity in the session.
Filters:
Time Since Start of Session is greater or Equal to 1 Day.”[32]

4. User IDs should not be shared or used by anyone other that the User to whom they are assigned. Users shall be accountable for all activity associated with their assigned User IDs. – Check for logged in ID’s over the time that the account should be active. Manual and spot checks to confirm that users do not leave the machines logged in when not in use.

The query of Accounts Logged in More Than one Day will help, but manual checks must also be done.

5. User IDs should be added, modified, and deleted in accordance with MHealth-approved account management processes.

   Check procedures and talk with the administrators as to how they do the process. If possible, they could use a tool to help with the templates and rules so that it will help automate the processes and leave less room for human error.

6. User IDs must be disabled within twenty-four (24) hours of notification of a status change (for example, termination or change in job). – This is a manual audit that will be checked through procedures.

   Check procedures and talk with the administrators and human resources as to how they do the process. If possible, they could use a tool to help with the templates and rules so that it will help automate the processes and leave less room for human error.

7. User IDs that are unused, dormant, or inactive for forty-five (45) days must be disabled. – This audit can be done by checking for User IDs that have not been logged in for over forty-five (45) days and confirming that they are disabled.

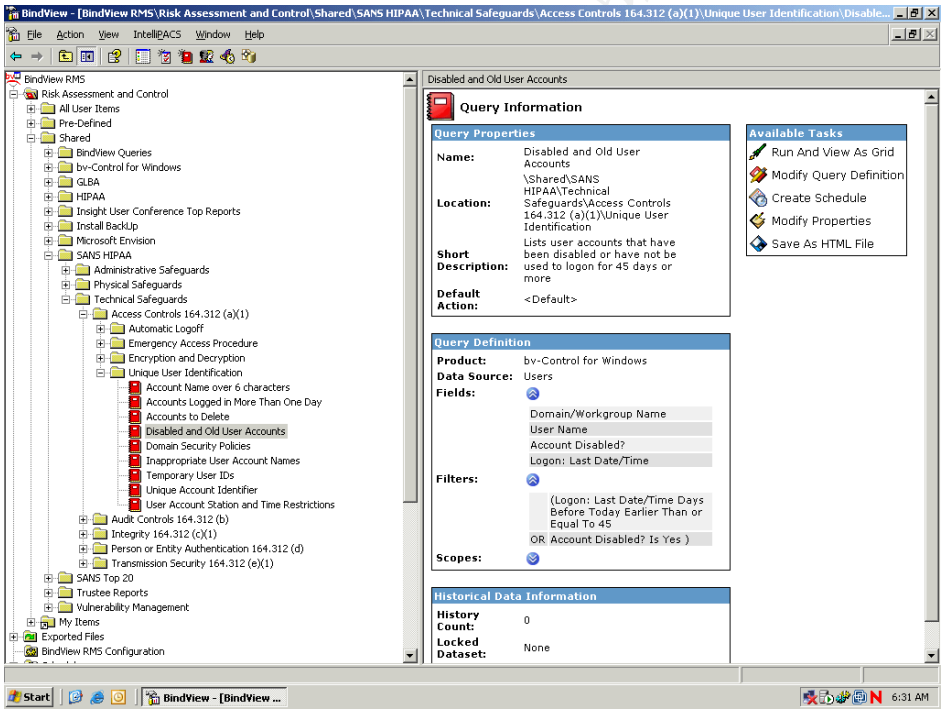

Figure 2: Disabled and Old User Accounts Query[33]

"bv-Control for Windows Query: Disabled and Old User Accounts
Data Source: Users
Fields: Domain/Workgroup Name: This field returns the name of the domain or workgroup that owns the user account.

User Name: This field returns the name of the user.
Account Disabled?: This field returns a “Yes” if the user’s account is currently disabled.
Logon: Last Date/Time: This field returns the date and time the user last logged into his or her domain.
Filters:
(Logon: Last Date/Time is 45 days or more from today OR Account is Disabled)
This filter will only bring back users that have not logged in for over 45 days OR if their accounts are disabled.”[34]

8. User IDs that are disabled for ninety (90) days must be deleted. – This audit will check for User IDs that have not logged in for over 135 days and are disabled.

“bv-Control for Windows Query: Disabled Accounts to Delete
Data Source: Users
Fields: Domain/Workgroup Name: This field returns the name of the domain or workgroup that owns the user account.
User Name: This field returns the name of the user.
Account Description: This field returns the Description in a user’s account definition.
Account Disabled?: This field returns a “Yes” if the user’s account is currently disabled.
Logon: Last Date/Time: This field returns the date and time the user last logged into his or her domain.
Filters:
(Logon: Last Date/Time is 135 days or more from today AND Account is Disabled)
This filter will only bring back users that have not logged in for over 135 days AND their accounts are disabled.”[35]

Check to see if in the procedures that they change the account description to include date that they disabled the account.

9. Temporary User IDs (for testing, contractors and temporary employees) should have an account expiration date that coincides with the anticipated end of employment, testing, or contract. –

This audit check is to check description of User ID to confirm that it has the words test, contractor, or temp within it. Audit check to confirm that there is an expiration date on this User ID.

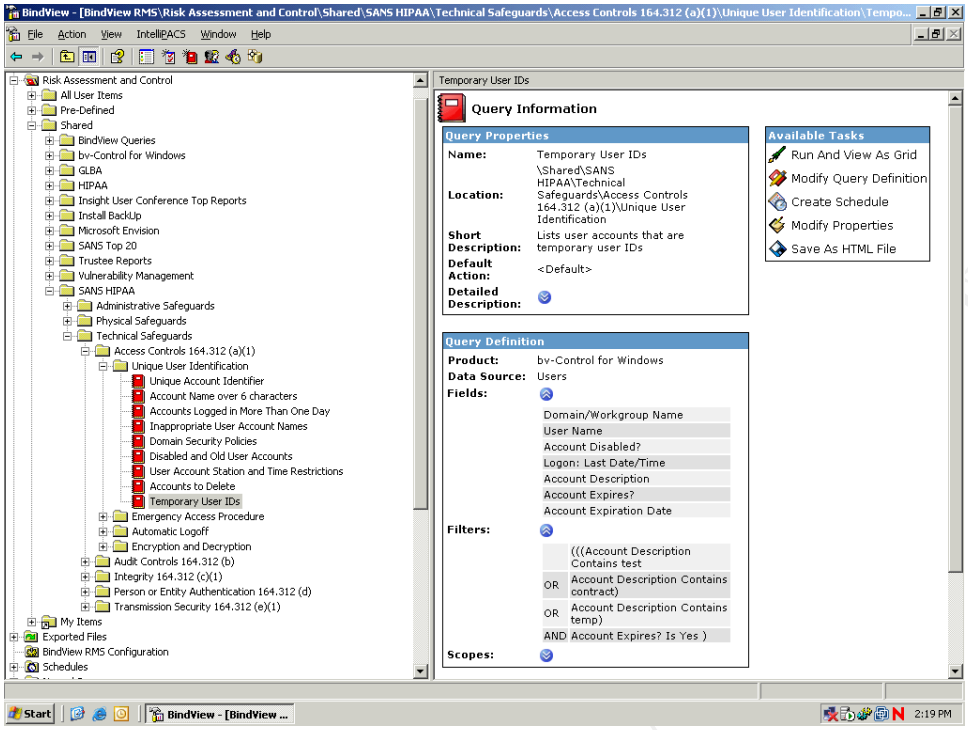

Figure 3: Temporary User IDs Query[36]

"bv-Control for Windows Query: Temporary User IDs
Data Source: Users
Fields: Domain/Workgroup Name: This field returns the name of the domain or workgroup that owns the user account.
User Name: This field returns the name of the user.
Account Disabled?: This field returns a "Yes" if the account is disabled.
Account Description: This field returns the Description in a user's account definition.
Account Expires?: This field returns a "Yes" if the account has an expiration date. "No" indicates an account that never expires.
Account Expiration Date: This field returns the date the user's account will expire.
Filters:
(Account Description Contains test OR Account Description Contains Contract OR Account Description Contains temp) AND Account Expires? Is Yes"[37]

IV. Analyze the results

It is not enough to run queries and get back reports, MHealth must also analyze the results. What does it mean to get back 15% of the User IDs that have not logged in for 45 days? Check with Human Resources to see if these users are still employed at MHealth, or is it that they are users that never use the system and do not need IDs, or possibly they are on leave.
Questions of "Why was there such a large number? Is there a large gap of

where you are to where you want to be? Do your policies fit the environment? Should they be changed? Is the 15% risk justifiable in your environment?" should be considered.

V. Notify responsible party

Once the results are analyzed, notify the people responsible. If there was a problem, check to see if the staff knew about and fully understand the policy, or if a breakdown in the procedures that caused this to happen.

VI. Assign remediation

By assigning remediation, you are attempting to correct the problem. This may entail changing the documentation to have new procedures, changing the User IDs, disabling old users, educating the administrators and users, and more. "CEs must regularly train employees and revise security policies and procedures as needed."[38]

VII. Certify/Recertify

Once you remediate the problem, re-audit the environment to make sure that it is corrected.

VIII. Repeat the cycle

Technology and regulations are continually being updated. Risk analysis may show that policies need to be changed. These eight steps should be a continual cycle to help keep your environment compliant.

References:

All BindView bv-Control for Windows Queries including report names, query fields, field information, sorting and scoping information:
"BindView RMS Console", BindView Corporation. Version 8.0.0.200. http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 8.0.0.200. http://www.bindview.com

"Policy Operation Center", BindView Corporation, http://www.bindview.com

"Sample Access Control Standard", https://policy.bindview.com/policy/6998, Policy Operation Center, BindView Corporation. 2005

"Assessment, Audit and Security", http://www.bindview.com/Products/VulnMgmt/AssessmentandSecurity/index.cfm, BindView Corporation

Ed Tittel, Mike Chapple, James Michael Stewart, CISSP: Certified Information Systems Security Professional Study Guide. Sybex Inc. 2003.

SANS Step by Step Series, HIPAA Security Implementation Version 1.1, The SANS Institute, 2004.

"What is CIS?" http://www.cisecurity.org/charter.html

"45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule", http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf, Federal Register / Vol. 68, No. 34 / Thursday, February 20, 2003 / Rules and Regulations

---

End Notes

[1] http://www.bindview.com/Products/PolicyComp/PolicyDevelopment/index.cfm, "Policy Development", BindView Corporation

[2] http://www.bindview.com/Products/VulnMgmt/Assessmentand Security/index.cfm, "Assessment, Audit and Security", BindView Corporation

[3] http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf "45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule", Federal Register / Vol. 68, No. 34 / Thursday, February 20, 2003 / Rules and Regulations, p. 46.

[4] Ed Tittel, Mike Chapple, James Michael Stewart, CISSP: Certified Information Systems Security Professional Study Guide. Sybex Inc. 2003, Page 149.

[5] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[6] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[7] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[8] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[9] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[10] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[11] SANS Step by Step Series, HIPAA Security Implementation Version 1.1, The SANS Institute, 2004. Page 206.

[12] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[13] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[14] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[15] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[16] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[17] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[18] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[19] https://policy.bindview.com/policy/6998, "Sample Access Control Standard", Policy Operation Center, BindView Corporation. 2005

[20] https://policy.bindview.com/policy/6998, “Sample Access Control Standard”, Policy Operation Center, BindView Corporation. 2005

[21] https://policy.bindview.com/policy/6998, “Sample Access Control Standard”, Policy Operation Center, BindView Corporation. 2005

[22] https://policy.bindview.com/policy/6998, “Sample Access Control Standard”, Policy Operation Center, BindView Corporation. 2005

[23] https://policy.bindview.com/policy/6998, “Sample Access Control Standard”, Policy Operation Center, BindView Corporation. 2005

[24] https://policy.bindview.com/policy/6998, “Sample Access Control Standard”, Policy Operation Center, BindView Corporation. 2005

[25] https://policy.bindview.com/policy/6998, “Sample Access Control Standard”, Policy Operation Center, BindView Corporation. 2005

[26] https://policy.bindview.com/policy/6998, “Sample Access Control Standard”, Policy Operation Center, BindView Corporation. 2005

[27] SANS Step by Step Series, HIPAA Security Implementation Version 1.1, The SANS Institute, 2004. Page 237.

[28] SANS Step by Step Series, HIPAA Security Implementation Version 1.1, The SANS Institute, 2004. Page 237.

[29] http://www.cisecurity.org/charter.html, “What is CIS?”, The Center for Internet Security

[30] “BindView RMS Console”, BindView Corporation. Version 8.0.0.200. http://www.bindview.com
“bv-Control for Windows”, BindView Corporation. Version 8.0.0.200. http://www.bindview.com

[31] “BindView RMS Console”, BindView Corporation. Version 8.0.0.200. http://www.bindview.com
“bv-Control for Windows”, BindView Corporation. Version 8.0.0.200. http://www.bindview.com

[32] “BindView RMS Console”, BindView Corporation. Version 8.0.0.200. http://www.bindview.com
“bv-Control for Windows”, BindView Corporation. Version 8.0.0.200. http://www.bindview.com

[33] “BindView RMS Console”, BindView Corporation. Version 8.0.0.200. http://www.bindview.com

"bv-Control for Windows", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com

[34] "BindView RMS Console", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com

[35] "BindView RMS Console", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com

[36] "BindView RMS Console", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com

[37] "BindView RMS Console", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com
"bv-Control for Windows", BindView Corporation. Version 8.0.0.200.
http://www.bindview.com

[38] SANS Step by Step Series, HIPAA Security Implementation Version 1.1, The SANS Institute, 2004. Page 3.