Securing Data & Delivering Value

Identifying Patient and Employee Related Sensitive Information in Data Repositories

Author: Rubensky Calixte, MBA, CISA

ahia
Assoc. of Healthcare Internal Auditors

Jackson
HEALTH SYSTEM

PUBLIC HEALTH TRUST

Table of Contents

Abstract

Healthcare organizations collect and store much more than just patient health information. Functional areas such as Human Resources, Internal Audit, and Finance accumulate terabytes of sensitive employee and patient information across business functions. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and National Institute of Standards and Technology (NIST) recommend guidelines to establish internal safeguards for sensitive data. However, operational and financial leadership, as well as Internal Audit, need practical solutions to identify and control the amount of and access to information stored within an organization.

This paper will provide insight into a practical framework through which internal auditors can economically identify sensitive information relating to both patients and employees in data repositories such as shared drives. Operational and financial leadership, Information Technology, and department data owners should use this framework to structure access rights and establish protective procedures. This whitepaper will provide an understanding of the tools and strategies needed to execute continuous security audits on corporate-wide sensitive patient and employee information.

How did we get to this point?

In 1928, Fritz Pfleumer patented the magnetic tape, ushering in the era of information storage. The advent of the hard disk in the 1950s enabled more efficient data storage and greater capacity. Floppy disks and compact discs (CDs) in the 70s and 80s made data mobile. Through the years, organizations have used many storage devices to store and secure sensitive data.

Throughout the evolution of data storage, from magnetic tapes to cloud storage, one constant remains: true security is a challenge. How do we keep stored information in the right hands? From the internal audit perspective, how do we effectively validate that the controls currently in place are truly adequate? What can your company do to ensure data is secure from both internal and external threats?

The Current Climate

In healthcare, the need to protect and audit the security of the data has never been more imperative. The advent of digital health records has raised the stakes; gone are the days when the tight security of medical records simply meant adding paper records into folders and putting them in a locked filing cabinet.

The potential exposure is also different. In the past, if a paper record was misplaced, stolen, or lost, the distribution of the record had limited geographical reach. The mere act of photocopying the records added a basic form of protection, due to the time and cost of illegal hand-to-hand distribution. Hackers anywhere in the world can now steal medical records and distribute the contents globally within seconds.

Today, clinical and business operations personnel are largely aware of the risks associated with inappropriate disclosure of sensitive information. IT personnel are more keenly aware of the risks and are committed to keeping sensitive information in the right hands. However, although IT departments can deploy software solutions, the clinical and business operations personnel play a much greater role in keeping data secure. As the actual owners of the data, they decide access rights and information storage location.

Over time, documents accumulate, records are modified in databases, and access rights change. Data owners may not understand which documents (or data elements) are no longer needed and which access rights are no longer required.

HIPAA is a Good Start

> **"Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation."**
>
> — Source: U.S. Dept. of Health & Human Services.

The U.S. Department of Health and Human Services (HHS) designed the HIPAA Privacy and Security Rules to be technology-neutral so the standards can remain relevant as time passes. This is a forward-looking approach, especially given the ever-accelerating pace of technological change. The flexibility within the Rules gives auditors room to incorporate different validation approaches. Elasticity can be a major plus, but the lack of specificity can leave many auditors unsure of which path will be most effective for their organization.

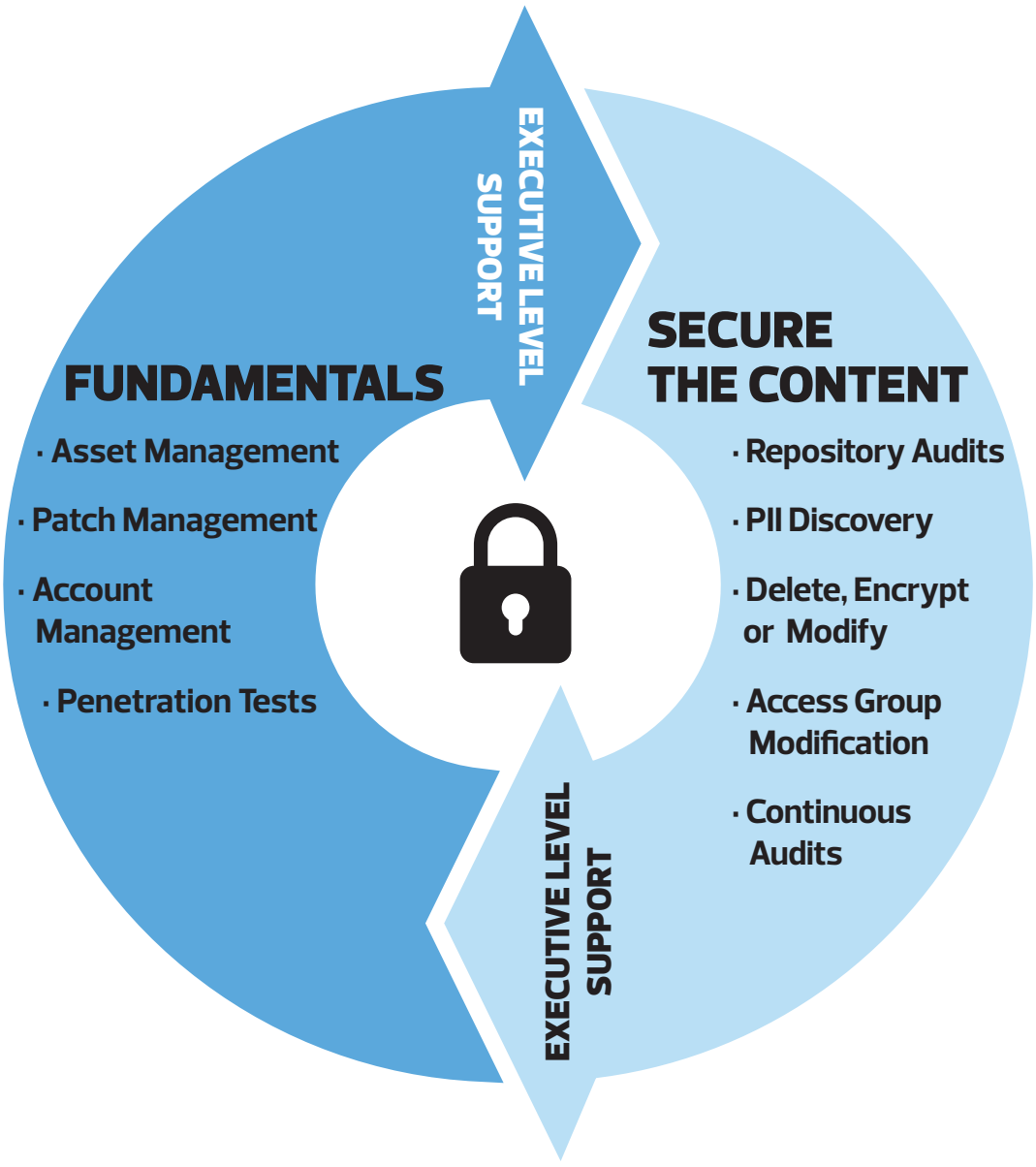
HHS also created a HIPAA Audit Program, which includes directives such as:

- "Evaluate and determine whether the technical implementation of the access controls used by the entity support the minimum necessary policies and procedures and are consistent with the Privacy Rule safeguard policies."
- "Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."

The directives alone are not specific enough to create fully developed audit programs leading to a material assessment of controls.

Auditors need strategies and guidelines which will continue to evolve as technology progresses. When it comes to auditing IT security and data repositories, there are certain fundamental truths **(Figure 1)** which auditors can implement to deliver valuable audits to stakeholders and stay relevant over time.

FIGURE 1



Fundamentals

Executive Level Support

Audit departments with a mission to deliver valuable IT security assessments need the full and clear support of the highest executive leadership. Executive support allows the audit process to move quickly throughout an organization and become a priority for department heads. This support is necessary for all types of IT audits, such as cloud computing assessments and soon-to-be-relevant blockchain audits.

Do not rely solely on internal audit charters or external engagements to drive executive support for IT security assessments. Sit down with the key decision makers of organizations, clearly explain security risks, and obtain their consensus to perform security assessments. These conversations pay dividends toward the latter parts of audits when potential roadblocks may arise, such as obtaining proper resources, validating findings with parts of the organization which may not understand the significance of IT audits, and ensuring proper follow-up.

Asset Management

Asset Management is the process of acquiring, maintaining, and disposing of assets effectively.

Organizations cannot truly control material aspects of IT security without getting asset management[1] correct. Without effective asset management, organizations cannot achieve optimal patch and account management. An organization cannot protect its assets without first knowing what it has. This inventory includes IT assets which may or may not be directly owned by the organization. A general rule of thumb is if the asset has any connection to the organization, the organization must continuously provide validation of the completeness and accuracy of the inventory. Whether kept in-house on the organization's network or managed off-site, an inventory of the assets is required.

A complete and accurate inventory listing of hardware and software enables patch and account management processes. The repository of assets should be properly logged to trace an asset back to its assigned location. Labeling standards should be documented and followed.

1. https://www.sans.org/reading-room/whitepapers/critical/leveraging-asset-inventory-database-37507

Patch Management

Patch management is an internal strategy for deploying critical security upgrades for software applications and technologies.

Identifying sensitive information and securing access rights in information systems both rely on an effective patch management program. For illustration, think of patch management in terms of a small physician's office with only physical paper, no electronic records.

The manufacturer of the file cabinets releases a memo stating that the cabinet locks are faulty. There is a way to bypass the lock without a key and all locks will be replaced at no cost. Most offices would have the locks replaced immediately. This situation is similar in the digital world; patches, upgrades and updates are frequently released to address security vulnerabilities.

The classic Microsoft hack, Conficker (or MS08-067), enabled hackers to gain admin-level access to information systems and essentially obtain all forms of information. Another similar hack, known as Wannacry, rendered systems useless through ransomware-based encryption. This hack targeted areas of the National Health Service (NHS) of the United Kingdom and infected over 300,000 computers worldwide. In both cases, Microsoft released patches that addressed the vulnerabilities months before hackers compromised those enterprise systems via the unpatched vulnerabilities.

Therefore, organizations must get patch management correct across all systems identified in the inventory listing to enable effective baseline security that reduces vulnerabilities.

Account Management

Account Management is the assignment and management of all accounts and logins associated with each system user and includes managing and removing access from former employees and contractors.

A south Florida healthcare organization suffered the repercussions of poor account management when the organization settled a HIPAA violation for USD 5.5M[2] for the unauthorized sharing of sensitive information through the system user account of a former employee.

System administrator access should be appropriately restricted and monitored. Management needs to establish mitigating controls to review and evaluate system administrator modifications.

Organizations must continually determine whether system usernames and passwords are correct and protected appropriately. Well-executed account management strategies and account audit programs help keep unauthorized individuals or groups out of internal networks. De-provisioning of access should be done timely and trending analysis should be performed to evaluate the process. This further ensures sensitive information is kept secure and protects the profits of the organization. Multifactor authentication is widely considered a good solution for safeguarding accounts.

---

2. https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html

Penetration Tests

Systematic penetration tests[3] are needed to gauge the readiness of an organization's security against a hacking incident. Penetration tests, done well, also provide validation of IT security initiatives including asset, patch, and account management programs.

A note on vendor management: The safeguards highlighted thus far also apply to third-party suppliers of information systems. Vendors should, at a minimum, perform asset, account, and patch management procedures to protect information systems and ensure patient safety.

3. https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Secure The Content

Identify Repositories

When the fundamental elements are in place or development, IT auditors can play an important role in assessing data repositories, such as shared/network drives. The first step is to identify each information system and assess the size of data stored within. This step is aided greatly by the asset management program.

Ideally, auditors would target and assess all data repositories and databases. However, many organizations lack the resources to take on such an effort in a continuous manner, and the overall returns (i.e., costs/benefits) from the review of smaller, lesser-utilized databases are likely low. A risk assessment that focuses on database content sensitivity and storage size is a good place to start.

Networked shared drives will likely rank high on most risk assessments. Many organizations use shared drives to store various forms of data across departments. Clinical and patient-related information, HR documents, and strategic initiatives are just some of the sensitive information most healthcare organizations are likely to have on shared drives. Documents which contain this type of information can accumulate over many years through onboarding and offboarding employees and contractors.

Often, data owners and operational managers are unaware of the sensitive data stored in share directories. Threats to this data can include a current employee who has access to a directory and decides to use discovered information inappropriately. External hackers also find loosely controlled file directories a key source to steal sensitive information.

Discover Personally Identifiable Information (PII)

Below is a step-by-step guide to finding PII in databases, identifying inappropriate users with access to the PII, and providing recommendations for remediation.

1. Assess Database Size

Once the decision is made on what data repository to target, auditors need to work with IT personnel to gain an understanding of the day-to-day operational activities and systems[4] associated with that repository.

[4] This paper presents solutions for Microsoft Windows based operating environments.

The auditor must gain an understanding of how storage is utilized in the repository. The activities and systems targeted will dictate the logical and staffing resources needed to execute the audit.

The auditor must also consider all tools and resources and how they work together. For example, Microsoft Windows-based PII tools programmed for Server Message Block protocol may not be compatible with a UNIX-based Network File System.

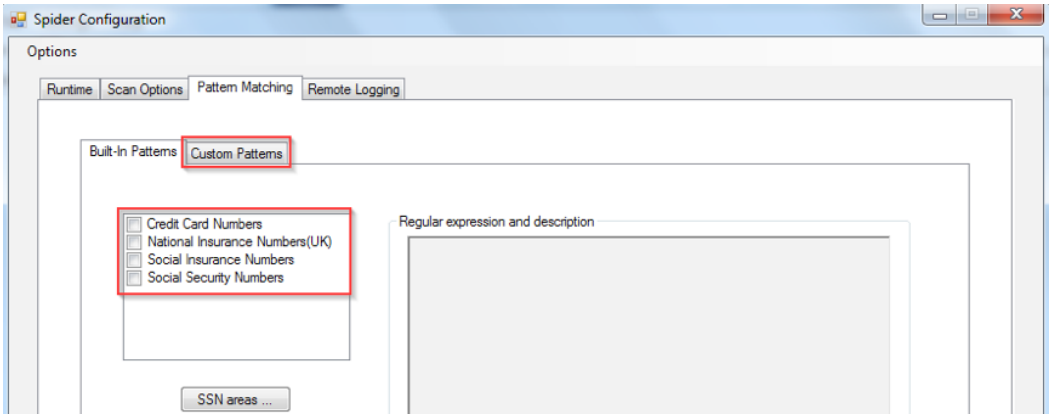
2. Acquire Tools[5]

Tools for PII Search (Where is the personally identifiable information?)

Start with a web search for 'PII Software' to understand the tool options available for PII discovery. For many organizations, budget considerations will dictate software selection. The price of PII discovery software can range from free to tens of thousand dollars (USD). Fortunately, for the economically-focused audit group, there are currently several good PII scanning software available at no cost.

One example of free software is CUSpider (a.k.a. "Spider"), created by Columbia University students[6]. It is simple and discovers social security numbers and credit card numbers. The software **(Figure 2)** is customizable to enable search queries for Employer Identification Numbers, National Provider Identifiers, Health Plan identifiers, and identifiers unique to specific providers/systems.

FIGURE 2

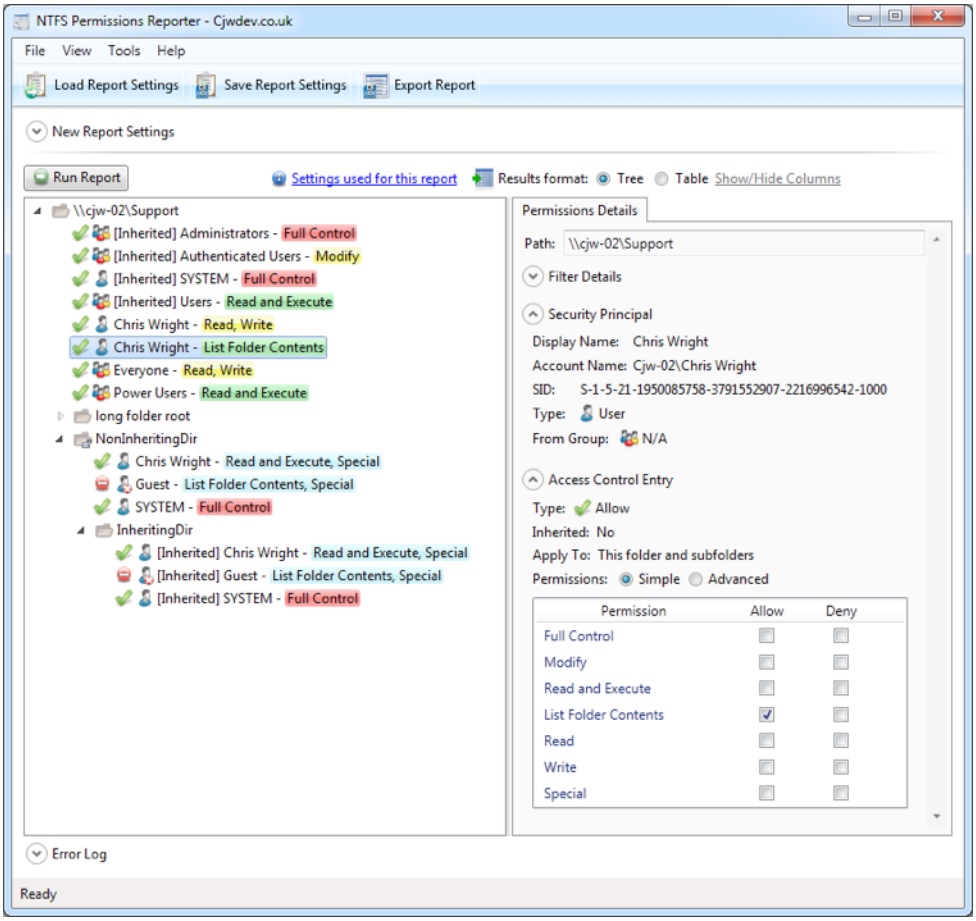


Tools for Access Search (Who has access to our data?)

There are many software tools available to perform access searches. An economical option is NTFS Permissions Reporter by CJWDEV, which has free and license-based versions available **(Figure 3)**. NTFS Permissions Reporter provides Excel outputs which include the names of users with access to directories, permissions assigned to users, and logical groups (used to assign multiple users to folders).

5. Auditors should obtain written permission from operational and IT leadership before utilizing software tools on corporate networks.
6. https://cuit.columbia.edu/cuit/it-security-resources/handling-personally-identifying-information/pii-scanning-software

FIGURE 3



[7]

3. Assemble Teams

To effectively complete this audit, an auditor must have a basic understanding of information systems and be comfortable navigating graphic user interface (GUI) software. Some PII and access search solutions require light programming, but these can be avoided by using GUI-based solutions. A team of at least two auditors to distribute workload is a good place to start; team size can be adjusted for the scope.

4. Computing Power

Auditors need to assess and determine how much computing power is needed to complete the audit. The more processing power utilized, the faster the PII and search software can complete queries. Processing power should inform the decision of whether to use the free or more expensive software.

7. http://www.cjwdev.co.uk/Software/NtfsReports/Ntfsv1-main.png

5. Read-Only Access

Internal Auditors should collaborate with IT administrators to secure read-only access to the file directory of the organization. Scanning entire file directories and access lists can take many hours depending on the directory size and the sophistication of the scanning tools. An auditor could rely on obtaining scan outputs from IT but having read-only access enables auditors to react to scanning errors and collect evidence in real-time.

6. Scan File Directories

CUSpider

For PII audits with strict budgets and timelines, consider running simultaneous sessions of the scanning tool. Virtual machines or multiple desktops/laptops with sufficient CPU and memory capacity are highly recommended.

For CUSpider, the scanning steps are as follows:

1. Target the directory and run the scan **(Figures 4 & 5)**
   a. Unselect options for scans of undesired directories

FIGURE 4

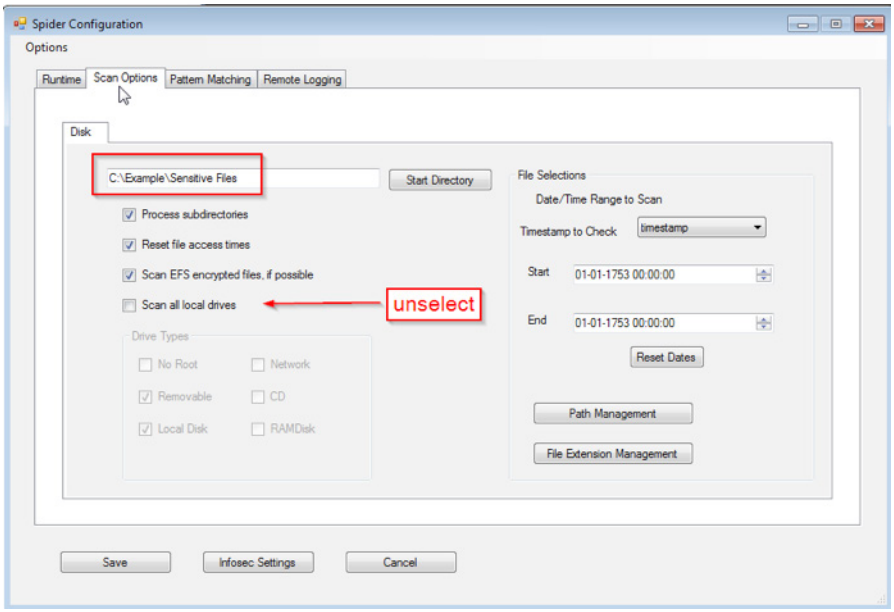
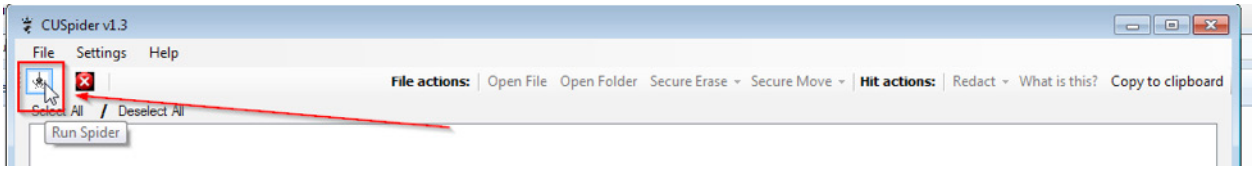


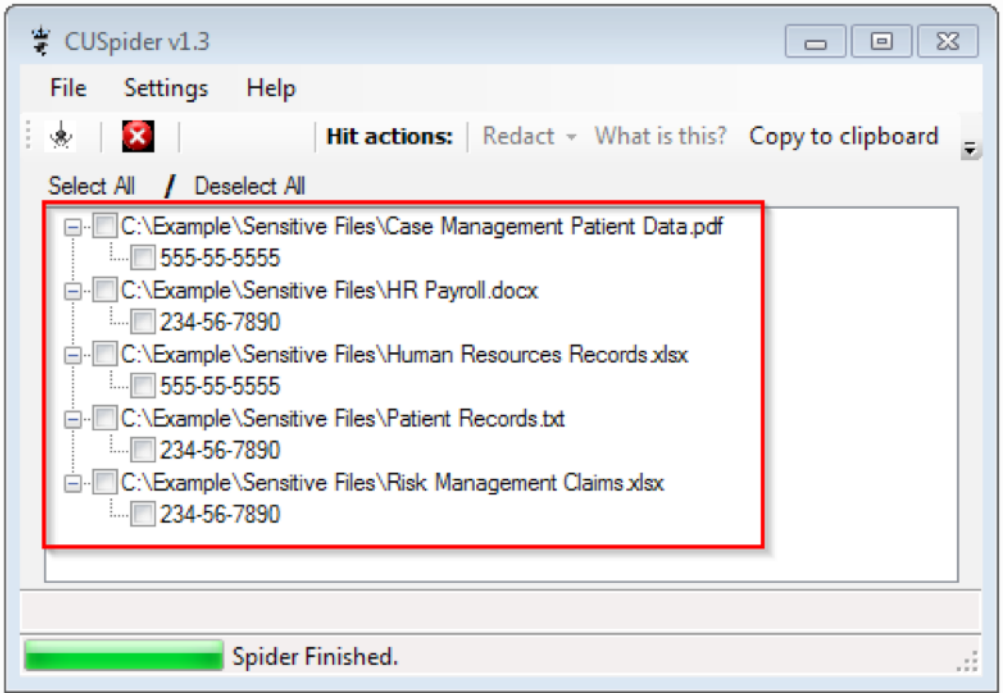
FIGURE 5



2. Collect results (Figure 6)

Most PII scanning tools allow exporting to Microsoft Excel, but some will only allow outputs specific to that particular software. Manual record-keeping via screenshots is a viable option for such cases.

FIGURE 6



Scanning Considerations

How to Handle Errors

Be prepared to handle application errors as problems arise. A 'set it and forget it' strategy is not a recommended course of action because many applications ask for user feedback when files are corrupt or in use. Lack of vigilance may unnecessarily prolong the timeline of the audit.

Keep Records

Keep detailed records of the PII identified so that analysis can be performed and trends can be highlighted. CaseWare IDEA, ACL, or Excel each can be used to bring forth value-added take-aways. At a minimum, the following fields/data elements (Figure 7) should be captured from the directory scanning software and entered into the desired data analytical tool: logical drive name/letter, the filename of supporting evidence, file directory identified as containing PII, and the number of files found.

FIGURE 7

	A	B	C	D
1	Drive Letter	Filename	Directory Location	Count of sensitive files
2	C	Supporting Evidence 1.xlsx (i.e., scanning tool output file, screenshot, etc.)	C:\Sensitive File Location 1\Employee Salaries\	2
3	G	Supporting Evidence 2.xlsx	G:\Sensitive File Location 2\Patient Billing Records\	7
4	P	Supporting Evidence 3.xlsx	P:\Sensitive File Location 3\Clinical Lab Reports\	4

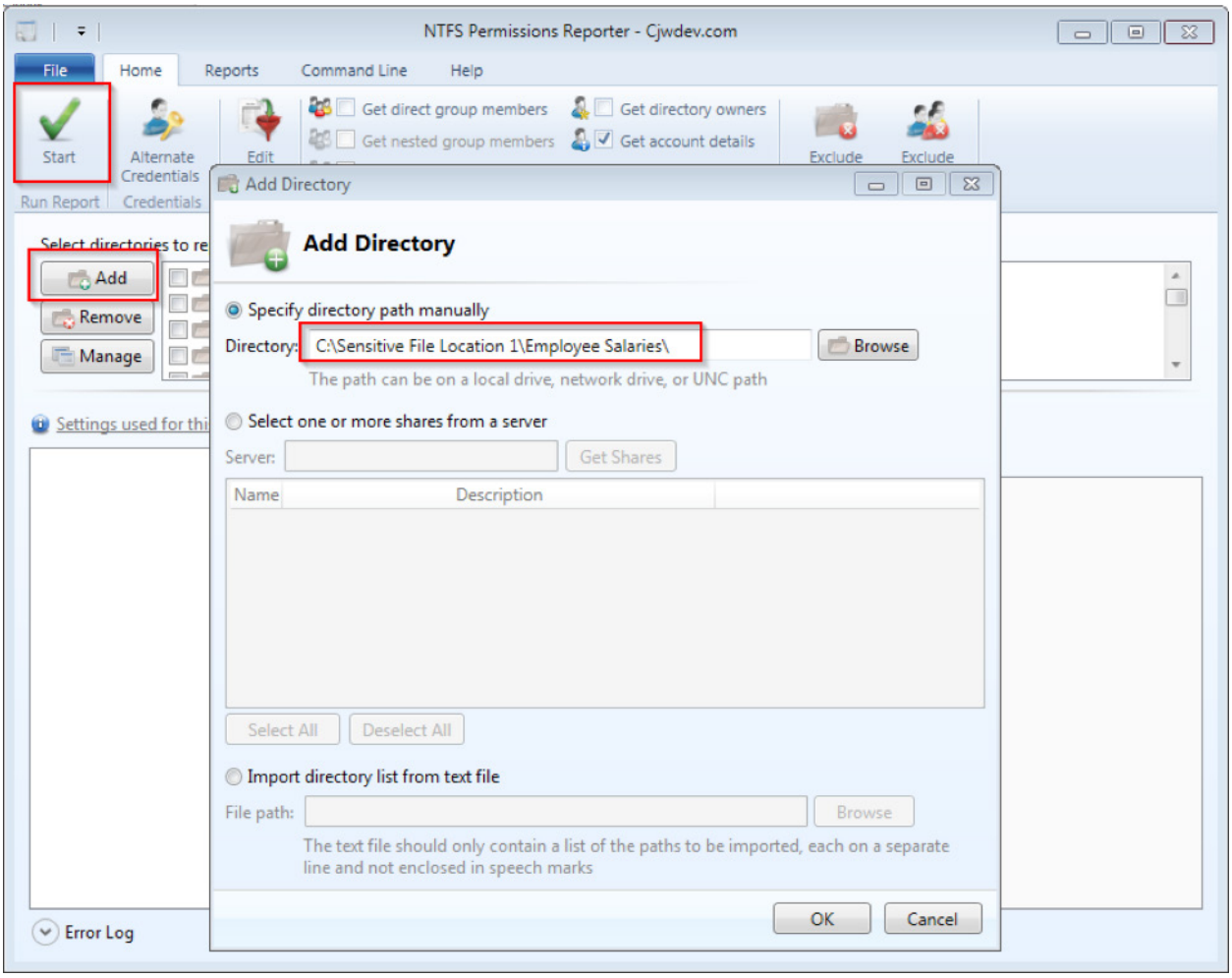
8. Scan for User Access

NTFS

For users of NTFS Permissions Reporter, the scanning procedures flow as follows:

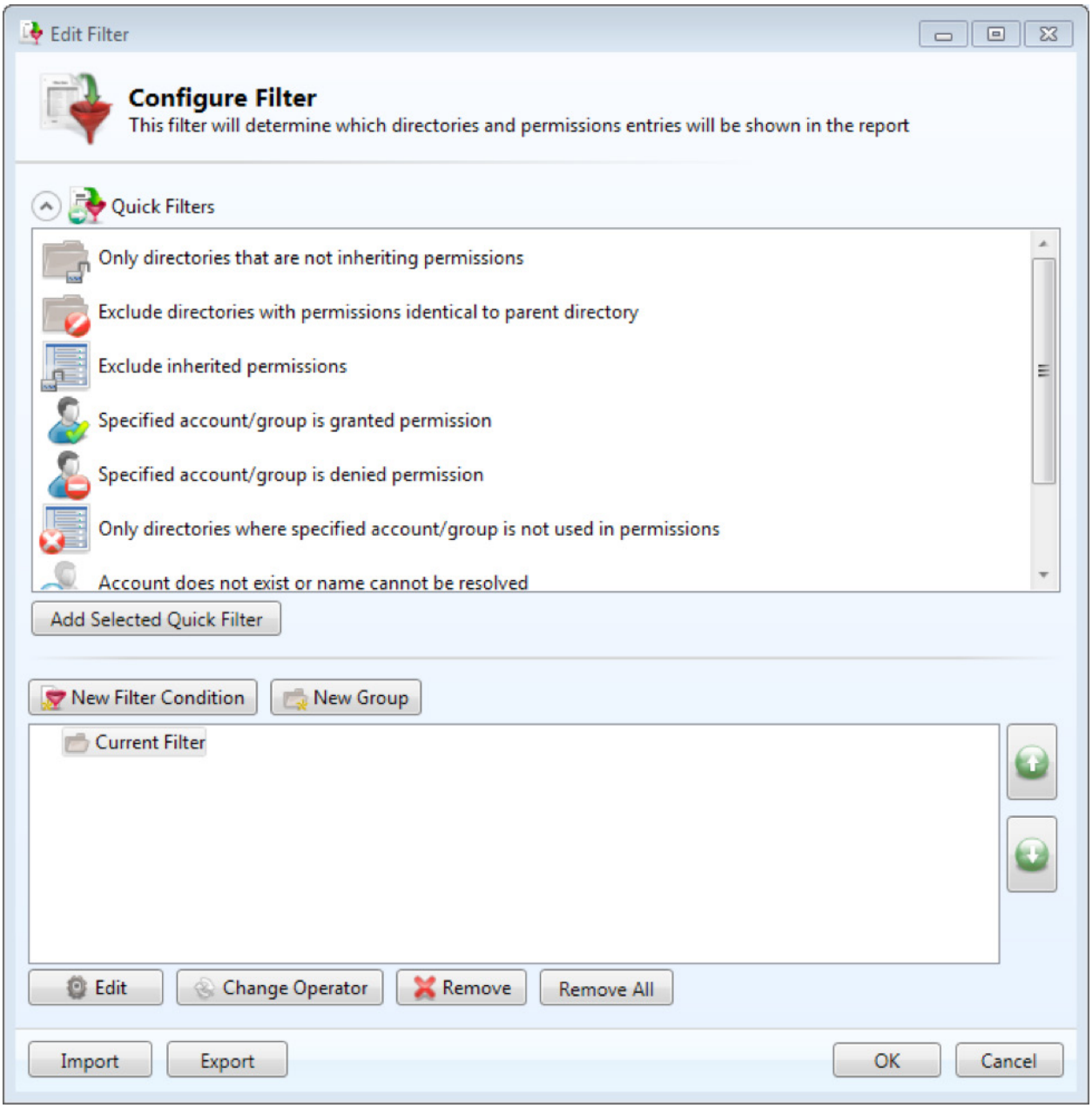
1. Select the target directory **(Figure 8)**.

FIGURE 8



2. Use filters to increase the speed of scans and to limit redundant information, if the scanning tool has this feature **(Figure 9)**.

FIGURE 9



3. Export the results to the desired software format. NTFS Permissions Reporter exports data in a native format and to Microsoft Excel **(Figure 10)**.

FIGURE 10

Cjwdev NTFS Permissions Reporter Export

Exported At: 10/5/2017 12:34 PM
Report Run By: Internal Audit
Excluded Directories: None
Filter: Directory inherits permissions is False

Path	Account	Account	Display Name	From Group	Permission
C:\Sensitive File Location 1\Employee Salaries\	User	HOSPITAL_DOMAIN\jdorian	Dorian, John	HOSPITAL_DOMAIN\HR_Employees	Modify
C:\Sensitive File Location 1\Employee Salaries\	User	HOSPITAL_DOMAIN\mgrey	Grey, Meredith	HOSPITAL_DOMAIN\HR_Employees	List Folder Contents
C:\Sensitive File Location 1\Employee Salaries\	Computer	HOSPITAL_DOMAIN\GenericAccount$	Account, Generic	HOSPITAL_DOMAIN\HR_Employees	Modify
G:\Sensitive File Location 2\Patient Billing Records\	User	HOSPITAL_DOMAIN\phawkeye	Hawkeye, Pierce	HOSPITAL_DOMAIN\Revenue_Cycle_Group	List Folder Contents
G:\Sensitive File Location 2\Patient Billing Records\	Group	WINDOWS_BUILTIN\Admins	Admins, System	N/A	Full Control
P:\Sensitive File Location 3\Clinical Lab Reports\	Group	WINDOWS_BUILTIN\EHR_Admins	Admins, HER	N/A	List Folder Contents
P:\Sensitive File Location 3\Clinical Lab Reports\	User	HOSPITAL_DOMAIN\dross	Ross, Doug	HOSPITAL_DOMAIN\Nurse_Practitioners	Read and Execute
P:\Sensitive File Location 3\Clinical Lab Reports\	User	HOSPITAL_DOMAIN\shardy	Hardy, Steve	HOSPITAL_DOMAIN\Physician_Group	Modify

4. Analyze the data. The main objective of the analysis is to translate data into an easy-to-understand language that aids decision-making. Before validating findings with data owners, auditors must analyze the data to satisfy the needs of the audit and to anticipate any questions or concerns from data owners and leadership.

   Once the location of sensitive documents and the individuals with access to this information are identified, auditors can combine the areas of information into a desired audit-testing program.

   At this point, auditors should have enough information to create a testing matrix **(Figure 11)** similar to the following[8]:

FIGURE 11

		Audit Procedures				
Information Collected From Scans		**1**	**2**	**3**	**4**	**5**
File Name(s):	Supporting Evidence 3.xlsx					
CUSpider Folder Path:	P:\Sensitive File Location 3\Clinical Lab					
Group Name(s):	*HOSPITAL_DOMAIN\Physician_Group*					
	Employee/Generic Account Name					
Individual Access:	Hardy, Steve	TBD	TBD	TBD	TBD	TBD

[8] TBD means "the results of the audit procedures are to be determined."

Auditors should obtain job descriptions from HR and, with the aid of audit tools, test the data collected. At a minimum, perform the following audit procedures to determine whether:

1. The job function of the user with access to sensitive data is in accordance with the intended purpose of the logical access group.
2. The user is a current employee or contractor.
3. Sensitive information access is appropriate: the user needs access to the respective sensitive information.
4. IT leadership and data owners approve generic accounts with access to sensitive information.
5. The location of the sensitive information is appropriate and correct.

9. Assure Quality and Validate Findings with Data Owners

Before validating findings with data owners, review the data for false positives. Scanning tools commonly flag mistyped phone numbers as SSNs, for example. Validating the findings with data owners can take much of the audit time-budget depending on the size of the organization and audit scope (i.e., sample testing vs. complete directory scans). The PII audit steps described, with complete directory scans, can take over a year or more to fully complete in a large organization. Plan accordingly.

Recommendations

There are three ways to remediate sensitive information/documents found within file repositories. The sensitive files can be deleted, modified/de-identified, or encrypted.

Delete (recommended)

Deleting sensitive documents[9] is an easy and quick approach to addressing discovered PII. The data owners, or IT personnel with the approval of data owners, can delete the sensitive file(s) altogether, thus mitigating possible inappropriate data exposures.

Encrypt

Encrypting the sensitive documents is a more moderate solution. Encryption involves locking the file and its contents behind a password or passkey and the files stay available for future use. Economically feasible tools[10], such as 7-Zip and VeraCrypt, enable users to encrypt individual files. Data owners can also move the sensitive files to an encrypted drive location separate from day-to-day (production) activity. Encryption tools feature several protection options, and NIST recommends methods such as Advanced Encryption Standard (AES), RSA public key cryptography, and SHA-256[11/12].

Modify

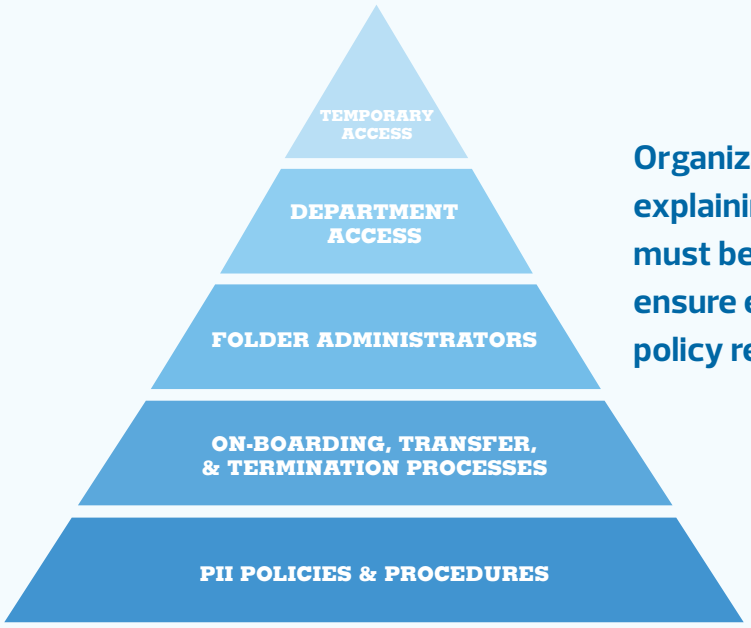
Modifying[13] the sensitive data set is the most time-consuming of the three remediation options. This method changes, hides, or masks sensitive information; for example, changing an exposed social security number (SSN), 123-45-6789, and modifying it to xxx-xx-6789 within documents.

Remediation steps can also include changes to access group permissions.

---

9. Consult legal counsel before implementing a deletion strategy. Organizations, such as public health entities, could be required to hold on to all forms of information for discovery purposes.
10. Auditors should obtain written permission from operational and IT leadership before utilizing software tools on corporate networks.
11. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
12. https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
13. Modifying the data set, which is deemed sensitive, is the most time-consuming of the three remediation options. This method entails changing or hiding some sensitive digital information.

Change Access Groups (Account Management)



Organizations should have clear policies explaining where sensitive information must be stored and require training to ensure employees fully understand policy requirements.

Changing the way folder access is granted may be necessary. There are three key areas of focus to support an optimal function of logical access over sensitive folder data: Corporate policy related to sensitive information; access controls over modifications to share drive access; and on-boarding, transfer, and termination processes.

Organizations should have clear policies explaining where sensitive information must be stored and require policy training to ensure employees fully understand policy requirements. IT Service Desk[14] processes should track and control requests for folder and logical access modifications. Onboarding, transfer, and termination processes must reconcile with and enforce corporate sensitive information policy for folder permissions.

Limit Folder Administrators

Folder administrators, the IT personnel with administrator access, should be limited to the IT department individuals with assigned responsibilities to service the day-to-day operational tasks and problems related to folder management. The size of the administrator group should be a fraction of the IT departmental staff.

Like lock and key physical filing cabinets, a physician's office should not give physical keys to a large number of staff members. Access must be limited to the point of absolute necessity. Also, administrative access provides the recipients with access to sensitive information, and therefore adequate training should be required for administrators.

14. The IT Service Desk process is responsible for resolving IT related requests and responding to incidents.

Identify and Manage Department Groups

Members of user departments will typically be the largest population with access to folders. IT personnel typically assign the department name as the title of shared folders to easily identify the purpose and owners of the folder. Department data owners should work with IT to ensure that on-boarding, transfers, and termination processes keep access rights appropriate.

Utilize Temporary Groups

Temporary logical access groups can be created and labeled with descriptive termination dates within the title to identify users who need temporary access (i.e., for projects). Using software such as NTFS Permissions Reporter, IT personnel can more easily identify temporary members and remove access promptly.

Perform Continuous Audits

The guidance given in this whitepaper can also be used by audit departments seeking to perform continuous audits. Using insights gained from a single review, auditors can perform more frequent audits to target directories with higher counts of PII and directories with known access control issues.

Audit teams can also invest in data analytics software, such as ACL or IDEA, to automate testing. Corporate data loss prevention software is an alternative for continuously identifying PII and other forms of sensitive information saved on data repositories.

Summary

Information Security in the healthcare industry has come a long way from the lock and key filing cabinet. Data storage methods will change over time. Data owners must control access rights and file security. Operational leadership needs practical solutions to identify and control information.

Functional areas such as Finance, Strategy, Human Resources, and Internal Audit can leverage common IT security practices aligned with HIPAA guidelines to make security gains. This guide provides organizations an economical method of auditing both patient-related and employee-related sensitive information in common data repositories.

Whether sensitive information resides in a small medical office or a large medical institution, these tools and strategies will help deliver insightful feedback to decision makers.

Author Biography and Contact Information

Rubensky Calixte is the IT Audit Manager at Jackson Health System (JHS), a nonprofit academic medical system. Jackson Memorial Hospital, a centerpiece of JHS, is the largest public hospital (by number of beds) in the United States. With over ten years of IT and Audit experience, Rubensky has provided assurance services to multiple S&P 500 companies. Rubensky holds an MBA from Babson College, a BS in Electrical Engineering from the University of Florida, and is a Certified Information Systems Auditor.

Email: rubensky.calixte@jhsmiami.org
Phone: 305.585.4330
https://www.linkedin.com/in/rubenskycalixte/

Acknowledgments:
Andre Reid, Vice President of Internal Audit, Jackson Health System
Eram Ahmed, Director of Finance, The Lennar Foundation Medical Center, University of Miami Health System

Additional Reference Links:

https://blog.varonis.com/4-step-guide-to-managing-network-share-permissions/

http://www.zetta.net/about/blog/history-data-storage-technology

http://www.techradar.com/news/computing-components/storage/the-data-capacity-gap-why-the-world-is-running-out-of-data-storage-1284024

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html?language=en

https://archives.un.org/sites/archives.un.org/files/uploads/files/ARMS%20Guidelines%20on%20Shared%20Drives.pdf

About AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities and design audit approaches. It is meant to help readers understand an issue, solve a problem or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content related to healthcare internal auditing that does not promote commercial products or services. **Interested? Contact a member of the AHIA White Paper Subcommittee:**

AHIA

Alan Henton, White Paper Chair
alan.p.henton@vanderbilt.edu

Mark Eddy
mark.eddy@hcahealthcare.com

Linda McKee
lsmckee@sentara.com

Debi Weatherford
debi.weatherford@piedmont.org

Deborah Mendel, AHIA Board Liaison
Deborah.L.Mendel@Medstar.net

ahia
Assoc. of Healthcare Internal Auditors

Jackson HEALTH SYSTEM

PUBLIC HEALTH TRUST