MDDX
RESEARCH & INFORMATICS

WHITE PAPER

IS YOUR ORGANIZATION AT RISK?

A FOCUS ON SPONSORS AND IMAGING CORE LABS

A self-assessment for GxP and HIPAA concerns

MDDX RESEARCH & INFORMATICS
580 California St, Floor 16
San Francisco, California 94104

T (800) 441-MDDX
F (866) 382-4696
info@mddx.com
www.mddx.com

INTRODUCTION

Historically, the regulatory concerns of imaging core labs were focused on FDA 21 CFR Part 11, audit trails, data backup, and software/hardware validation. However, within the last several years, changes in federal regulatory auditing frequency and standards have created an additional area of focus. With the evolution of HIPAA through the HITECH Omnibus Final Rule, the burden of HIPAA compliance has expanded to include contracting organizations, holding them directly accountable. Sponsors now share liability for the compliance of their downstream vendors and subcontractors, including: maintaining best practices, record retention policies, and privacy and security measures.

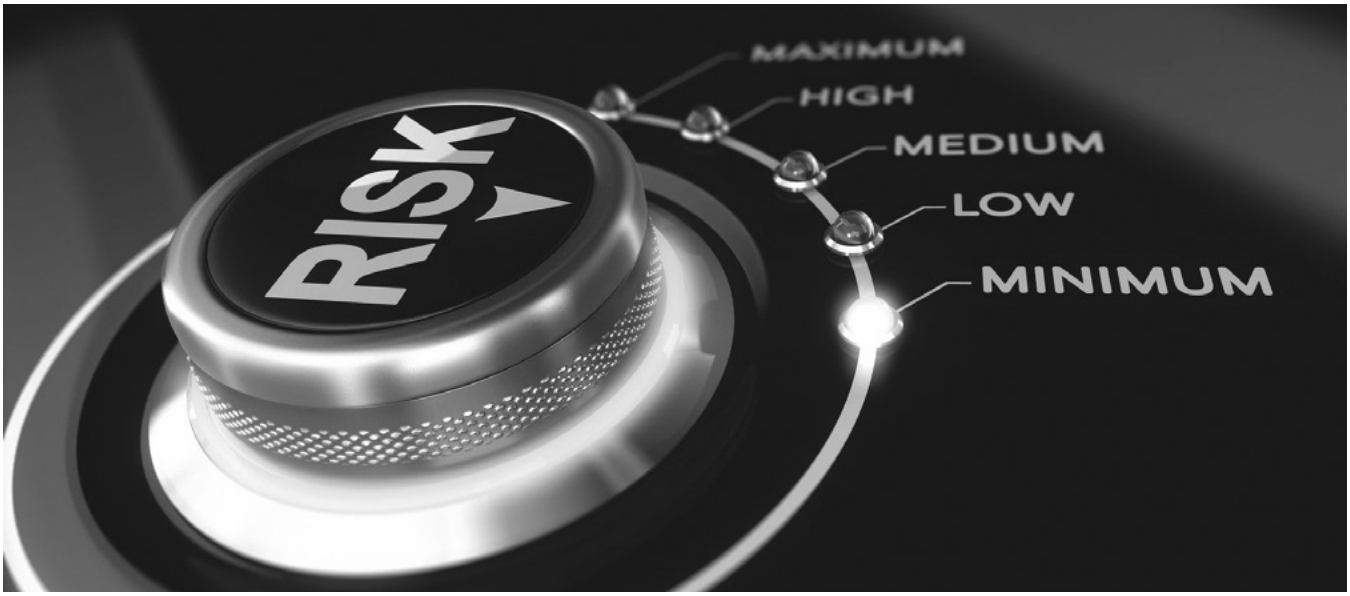
The Department of Health and Human Services' announcement that they will begin performing proactive audits of entities (especially business associates and subcontractors) has sent a clear warning to every organization that handles or has access to PHI: become compliant and be prepared for an audit.

HIPAA violations are often met with expensive fines and even potential criminal prosecution. The Office of Civil Rights has now given the State Attorney General the independent authority to investigate and prosecute these violations.

Under HIPAA standards, the de-identification of images requires stringent and complete removal of specific identifiers, however this removal must also be performed without interrupting the audit trail, chain-of-custody requirements of the FDA, or damaging the integrity of the image itself.

Every violation has the potential to subject the Lab or Sponsor to a $50,000 fine, even if the disclosure was unintentional and limited to a single document. Additionally, violations can result in the invalidation of trial data and, potentially, the discontinuation of an entire trial. These type of violations are embarrassing and avoidable.

Due to the increased risks and liabilities of running clinical trials, Sponsors and Labs are now reworking and bolstering their quality management systems as well as their overall handling of imaging data and potential sources of PHI.



RISKS TO SPONSORS AND IMAGING LABS

FOR LABS THAT RECEIVE IMAGES THAT ARE NOT DE-IDENTIFIED:

CATEGORY	RISK	DESCRIPTION	IMPACT
Incomplete or improperly de-identified images	HIPAA Violation – intentional disclosure	The lab is responsible for the downstream handling of all data. A notable percentage of HIPAA violations follow intentional disclosures by disgruntled employees — potentially years after the data was received.	Financial: $10,000 — $50,000+ per violation. Additional criminal penalties can apply. Notification of violation to affected individuals.
	HIPAA Violation — unintentional disclosure	Accidental disclosures resulting from lost or stolen laptops, thumb drives, and mobile devices	Financial: $100 — $50,000 per violation. Notification of violation to affected individuals. Typical OCR monetary penalties in HIPAA settlements **average $1,070,585.** *Recent Fines:* $2.75M to U-Miss Medical Center for theft of unencrypted laptop containing PHI. $650K to Catholic Health Care Services for theft of mobile device containing PHI
	Violation of Institutional Policy	Labs inside hospital or university settings are typically required to meet institutional privacy policies. The majority of US health centers do not allow identifiable health information unrelated to their patients inside the facility.	Occupational: Potential damage to professional reputation at primary place of employment
	Not blinded read	Most trials call for “blinded reads”, in which the lab does not know the identity nor source of the images. When DICOM are not fully de-identified, they display this information within their images or metadata. This violates the “blinded reads” requirement and risks involving a reader’s bias.	Potential professional embarrassment if sponsor’s competitors or governmental agencies highlight the discordance between the protocol requiring blinded reads and the potential for bias when non blinded reads have been performed.

FOR LABS THAT RECEIVE IMAGES THAT ARE DE-IDENTIFIED BY THE SITE:

CATEGORY	RISK	DESCRIPTION	IMPACT
Improperly de-identified images	Patient Mix-up	During the de-identification of multiple images during a single session the probability of mixing up images grows exponentially.	Treatment decisions based on incorrect images can result in patient injury or death. Even if the lab was not held directly liable they would certainly be implicated throughout onerous legal proceedings requiring rigorous defense.
	Absence of audit trail	Improper de-identification methods do not create the required audit trails which track the pre vs post changes of critical data fields, such as image counts or other DICOM tag values.	21 CFR Part 11 violation. Potential investigation and sanctions by FDA. This can also result in the data from those subjects being invalidated from the trial and even the lab being banned from future clinical trials.
	No chain-of-custody	Proper de-identification provides backtracking from the original source images to the final interpretation, ensuring that the correct images were interpreted and that no improper data modifications occurred (intentional or accidental) that could skew the results.	Can result in the data from those subjects being invalidated from the trial and even the lab being banned from future clinical trials.
	HIPAA Violation	HIPAA requires that a specific set of identifiers be removed for the data to be considered de-identified. Images that are de-identified by the site or lab rarely meet these standards.	Labs often live under a false sense of security that they are low-risk because they don't use patient names. However, improper de-identification results in only removing "surface level identifiers", while numerous less obvious identifiers remain inside the images and metadata. By unknowingly sitting on identifiable images, labs may actually be liable for all of violations list above.

SELF-ASSESSMENT

Please answer each of these questions as related to your imaging handling between the sites and the imaging core lab:

PART A: *Please answer the questions below by circling the answer that fits best*					
Does the lab follow a protocol identified in a signed SOP that controls the proper de-identification of medical images to meet HIPAA/HITECH standards?	Never 3	Sometimes 2	Mostly 1	Always 0	Unknown 4
Does the lab ever accept images or see data that contains patient initials, date of birth, the institution name where the images were acquired, or other individually identifiable health information?	Never 0	Sometimes 2	Mostly 2	Always 3	Unknown 4
Does the lab ever accept images that are not fully de-identified?	Never 0	Sometimes 2	Mostly 2	Always 3	Unknown 4
Are there trial-related images being stored in the lab that meet the following:					
- Stored on an encrypted hard drive on a device that has been fully validated	Never 4	Sometimes 4	Mostly 4	Always 0	Unknown 4
- Access limited to specific individuals with documented training in patient privacy, 21 CFR Part 11 and data security	Never 3	Sometimes 2	Mostly 2	Always 0	Unknown 4
- Have all identifiers been removed	Never 3	Sometimes 2	Mostly 1	Always 0	Unknown 4
Does the lab track all access to images to guarantee protection from tampering?	Never 3	Sometimes 2	Mostly 1	Always 0	Unknown 4
Has the lab documented that all images are encrypted during transmission?	Never 3	Sometimes 2	Mostly 1	Always 0	Unknown 4
TOTAL FOR PART A					

PART B: *Please answer the questions below*					
Tractability/Chain of custody: Does the sponsor or lab have a protocol to ensure that the identity of the interpreted images can be traced back to the original images at the source hospital?	Never 4	Sometimes 3	Mostly 2	Always 0	Unknown 4
Does the lab have protocols which ensure that other sponsors' data is not visible to their competitors during an audit?	Never 3	Sometimes 2	Mostly 1	Always 0	Unknown 4
Does the lab have an ironclad method to demonstrate that the reader who signs the interpretation report is indeed the actual reader (i.e. not a tech or fellow doing the read for them)?	Never 4	Sometimes 3	Mostly 3	Always 0	Unknown 4
Has the lab documented the following (even if part of a larger institution where some of these functions are centrally provided): - The delineation of facility security vs lab security - A named individual (internal or external) listed as the privacy and security official **Privacy and Security Officer** - Record keeping methods - Access and identity verification procedures	Never 4	Sometimes 3	Mostly 1	Always 0	Unknown 4
Has the lab performed an internal audit to assess that all of the above data integrity and privacy measures are met?	Never 4	Sometimes 2	Mostly 1	Always 0	Unknown 3
Has the sponsor or proxy performed an external audit to assess that all of the above data integrity and privacy measures are met?	Never 4	Sometimes 2	Mostly 1	Always 0	Unknown 3
TOTAL FOR PART B					
TOTAL COMBINED SCORE FOR PARTS A AND B					

Total Combined Score: _____

SCORE RANGES AND INTERPRETATION:

0-10	10-22	23 – 31	32+
EXCELLENT	**AVERAGE**	**BELOW AVERAGE**	**PROBLEMATIC**

INTERPRETING YOUR SCORE:

EXCELLENT: You have greatly reduced or eliminated the majority of risks and liabilities. There is a high likelihood that your organization will pass an external audit with little or no findings.

AVERAGE: Your organization has implemented the majority of procedures required to attain an EXCELLENT score, however there remain a few minor items or unknown items that must be addressed to pass an external audit.

BELOW AVERAGE: There are aspects to your operations that are currently subjecting your organization to considerable risk and liability. You have completed a significant portion of the requirements; however, the gaps leave you very exposed. Many auditors could be particularly harsh on this sort of patchwork compliance system. You have shown that you know enough to understand the regulations but have failed to consistently implement them. Risks can range from having research data invalidated or stolen to financial penalties for privacy violations.

PROBLEMATIC: Most of the scores we see in this area are from organizations that have selected "unknown" for many of the questions. This puts you and your organization at the highest risk. It is a legal requirement that key members of your staff or designated third party providers know and understand the requirements. Immediate preventative and corrective actions must take place in order to avoid potentially catastrophic liability should a breach occur.

For each NO answer in Part A, the labs chance of being cited for a HIPAA/Privacy breach increases exponentially. Being digital, DICOM images are easy to copy, transport, and lose — thousands of images can fit on one thumb drive. it should be clear why every image containing patient identifiers creates multiple chances for a privacy breach: Most labs have multiple staff members, high case traffic, and frequent staff turnover (due to medical trainees) in an environment without stringent data containment methodologies and record retention regulations.

Even if the Sponsor is found directly liable for a privacy breach, in the event that a multi-million dollar fine is issued, the party subject to these fines is likely to seek damages from all other parties sharing the liability. This liability is likely to reach the lab when the sponsor cites arrangements for the transport of the images to the lab that contained identifying information.

For each NO answer in Part B, the sponsor's risk of having trial data invalidated by the FDA increases significantly. If data tractability via audit trails of pre- and post-de-identification cannot show traceability between the original patient and the analyzed images, then that subject's data will be invalidated from the trial. As the sponsor is also responsible for FDA 21 CFR Part 11 compliance of the lab's data handling, FDA violations can be targeted at both the sponsor and lab. Penalties range from minor violations to data being invalidated to those institutions being barred from future clinical trials, while also including product recalls due to data integrity issues.