Security and Privacy: An Introduction to HIPAA

A Paper by:

The Privacy and Security Committee

Medical Imaging Informatics Section

February 14, 2001

Security and Privacy: An Introduction to HIPAA

Security and Privacy: An Introduction to HIPAA

1. Introduction to the Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed by President Clinton on July 21, 1996 and has the general objectives to

- Guarantee health insurance coverage of employees.
- Reduce health care fraud and abuse.
- Introduce/implement administrative simplifications in order to augment effectiveness and efficiency of the health care system in the United States.
- Protect the health information of individuals against access without consent or authorization.

Within HIPAA there are Administrative Simplification regulations that, in early 2001, are in work.

The HIPAA Security and Electronic Signature Standards Notice of Proposed Rule Making defines security measures to be implemented in healthcare. This white paper gives an explanation of how this rule and the final rule about privacy of individually identifiable health information that became law on December 28, 2000, impact the medical imaging world.

This document is intended for educational purposes. It does not contain concise definitions nor mandatory guidelines, but instead outlines the main components of HIPAA that affect medical imaging equipment.

2. How HIPAA Affects the Health Care Sector

Covered Entities (CEs) as defined by HIPAA are health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with certain standard transactions. These CEs need to support many different data formats and protocols. Having only a single set of data formats and protocols will simplify administration. HIPAA defines standards for a set of transactions conducted in electronic form while still allowing any non-standardized paper form for these transactions. The proposed security standard would apply to all health information that is electronically maintained or electronically transmitted. The approved privacy standard applies to individually identifiable health information transmitted or maintained in any form, oral, written or electronic – called Protected Health Information (PHI). There are other regulations pending that deal with National Provider ID and National Employer ID; additional regulations will be proposed on National Health Plan ID, Claims Attachments, and National Individual Identifiers. We should think of HIPAA as an ongoing process to standardize the digitalization of health care information within the United States.

The United States government realized that by mandating patient records be sent over digital networks there would be fear that patient privacy could be compromised. To address this fear the Department of Health and Human Services developed a standard set of security and privacy regulations to which the above-mentioned CEs must adhere. As of this writing in February 2001 the latest published HIPAA regulation covers privacy of patient healthcare data. The privacy

regulation gives patients specific privacy rights, and defines specific rules, e.g., for health care providers on how these rights must be protected.

In order for a healthcare facility to protect privacy a set of security measures must be put into effect. In general, the healthcare industry has not focused on providing security and privacy features in their products. Health care providers, health care clearinghouses, health plans and insurance companies, and medical equipment and medical system vendors have all directed their efforts to treating the patient. Ethical considerations, whether codified in law or mandated by tradition, have governed the sharing of patient data. So what does this mean to healthcare and the vendors that serve it? It means that formal security and privacy practices and technologies will now need to be a part of the way these entities act and the products they develop.

CEs are required to become HIPAA-compliant. HIPAA compliance is not simply purchasing new HIPAA-compliant systems. Becoming HIPAA-compliant means to combine the security functionality that technology can provide with appropriate policies and procedures, as illustrated in Figure 1. Organizations must now assess risks and develop, document, implement and maintain appropriate security measures to keep risk at an acceptable level. These security requirements will include a combination of administrative and technical measures covering four broad categories: administrative procedures, physical safeguards, technical security services, and technical security mechanisms.

A good example of a technical security mechanism is "user identification". A system that has strong security measures built into it and that allows implementation and management of user passwords is not necessarily HIPAA-compliant unless strong policies and procedures are also in place to govern their use. No amount of technology can prevent a helpdesk operator from granting unauthorized access to a network by resetting a password, if an outsider can simply call in masquerading as an employee that has forgotten its password. Likewise people that commonly write

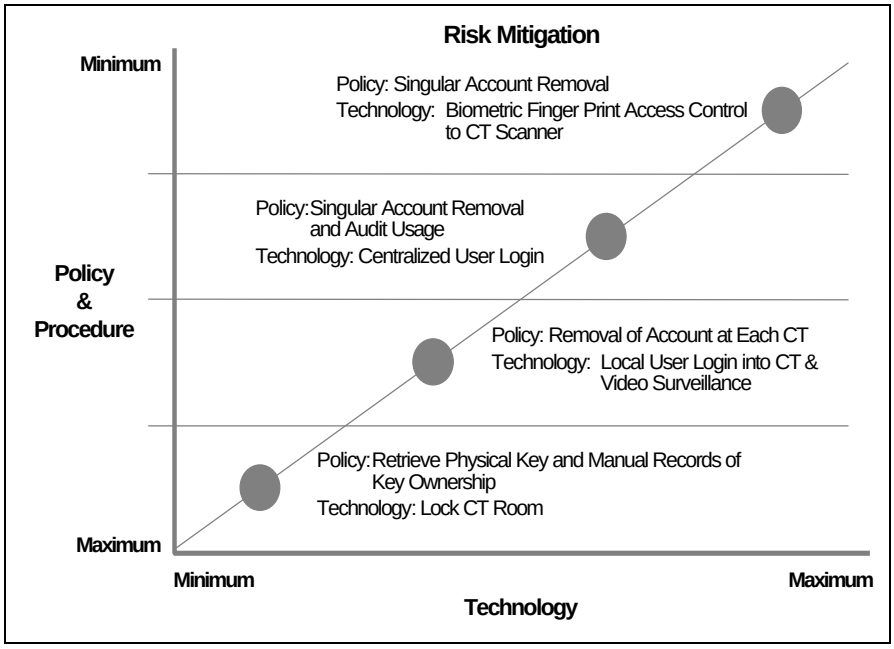

Figure 1: As This Example of an Employee Termination Process Illustrates, HIPAA-Compliance is a Combination of Processes and Technology, Since No Product Can Provide HIPAA-Compliance by Itself.

down their password, attach a note with their password on it to their monitor or tell others their password can defeat the best password-protected systems.

> CEs only become HIPAA-compliant by putting policies and procedures in place and requiring them to be enforced and followed.
> *No vendor can make HIPAA-compliant products*, but products can be made that make it easier for CEs to comply with HIPAA.

HIPAA is scalable. Each CE needs to perform a *risk assessment* and develop a plan to mitigate each and every risk discovered. This plan may include new policies, new procedures, AND new technologies. The vast majority of risks will be addressed by implementing new or revising existing policies and procedures to include items such as: moving PCs to more isolated locations, changing password policies, locking doors, etc. The specific plans at each facility will scale according to their needs. A small clinic may be able to address HIPAA with a much smaller plan than the large regional medical centers might need.

Risk mitigation is a moving target. HIPAA stresses that risk assessment and mitigation planning is a continuous process that needs to be reviewed often, with a new plan developed and implemented based on new threats and technology. What is reasonable today might not be acceptable tomorrow.

HIPAA specifically points-out that patient care cannot be affected. This is a very important aspect of the legislation since the most important thing CEs must do is take care of their patients.

HIPAA affects more than the CEs. Health Care Providers and other CEs are not isolated entities; they rely on many other services. Some examples of these services are ASP (Application Service Providers, which are 3rd party providers operating information systems located remotely but hosting data of the hospital and its patients), VPN (a Virtual Private Network can extend a hospital private network in a secured manner over a public network), outreach, and vendor remote or 3rd party remote servicing of hospital equipment. For each of these outside service providers, Business Associate contracts will need to be created and put in place. These contracts in essence extend some of the HIPAA regulations and make them applicable to the Business Associates themselves.

HIPAA does have some specifics that are spelled out in exacting detail, such as unique user identifications for each operator, auto logoff, audit trails of certain disclosures of patient data, virus checking, backups, disaster recovery, compliance audits, testing, training and optional encryption and digital signatures. The regulations, especially the proposed security regulation, are a framework and those governing each section of the framework must be met in some way. This could be through changes in hardware, software, or implementation of policies and procedures, or a combination.

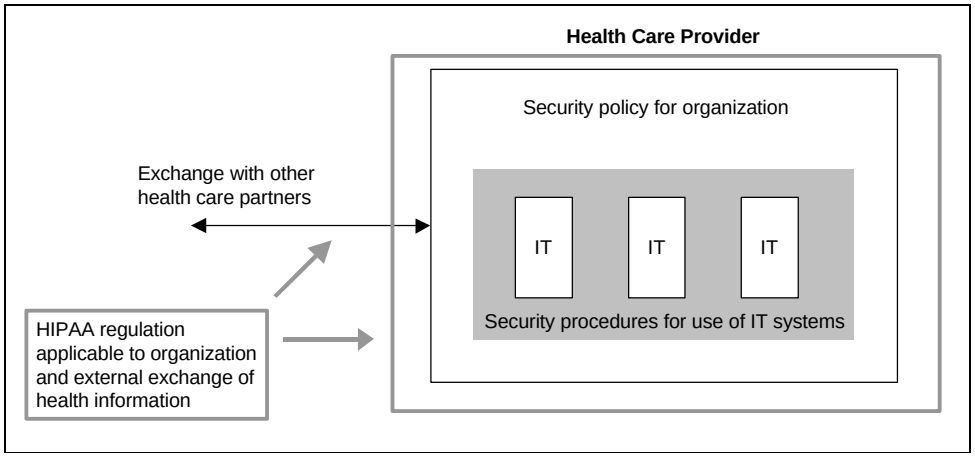

Figure 2: HIPAA Governs Sharing of Protected Health Information Accessed Within a Health Care Provider's Enterprise or Communicated to a Business Associate

Security measures for medical equipment must fit the directives and procedures of the typical healthcare provider, as illustrated in Figure 2. Physical security and organizational issues, e.g., procedures to gain access to systems and data, safe storage, detecting violations of rules, are outside the scope of medical equipment. However, medical equipment must provide the means to support these capabilities. On the other hand, medical equipment has to co-operate with other systems that implement part of the security solution, such as encryption key management systems and centralized authorization systems.

It is important to note at this point that security and privacy concerns do not only exist in the United States. There are long established personal data security and privacy regulations in Europe and Asia. While these regulations are not necessarily specific to the healthcare marketplace, they deal with similar issues.

3. Privacy and Security Concepts of HIPAA

Data privacy deals with controlling who is authorized to access information. The privacy regulation defines very specific rights that patients have. In order to maintain the privacy of a patient's PHI, required security measures need to be implemented. In this light, security services that need to be implemented in medical technology are concerned with the ability to control access to it, protect it from accidental or intentional disclosure to unauthorized persons, and guard it against unauthorized alteration, destruction, or loss.

CEs have experience with dealing with paper and film. Similar care is needed with electronic information. To increase the security provided for electronically handled information different measures are required. These can be split into a number of security services that are well-known in the security engineering community, i.e., confidentiality, integrity, and availability.

3.1 Confidentiality

The most fundamental function of security is to guarantee that information is used by or disclosed only to authorized individuals. Measures need to be implemented that grant access only after the person requesting the information has been properly identified and authenticated. The access rights of each individual must be restricted to only the information they need to know or

to the functions they need to do in order to perform their job, yet this restriction must not interfere with proper care of a patient.

Confidentiality can be implemented in various ways, from a physical lock on the door where the information is stored to stronger authentication procedures when physical access cannot be restricted. Unprotected and unattended logged-on workstations must be avoided because they can lead to compromise of PHI, plus personal and institutional liability and sanctions.

The need to protect the confidentiality of PHI also applies to data transmitted between equipment and systems. Physical protection of the communication path might suffice to thwart an eavesdropper within the physical confines of an enterprise. However, when PHI is to be exchanged over public networks then specific technology, such as encryption, will need to be employed to protect against compromise.

A specific mechanism, termed de-identification in the privacy regulation, can be used to remove enough information so the risk of identifying the patient to which the information belongs is very small. When PHI is properly de-identified, careful tracking of the data is no longer necessary. De-identification is not an exact science. Regardless of the means used to de-identify data, there remains a possibility that an individual can still be identified based on other available information.

3.2 Integrity

Systems that handle electronic information have to ensure that unauthorized modification to the information cannot be made without being noticed. Any time information is used or electronically communicated there needs to be a high confidence that the information is accurate. As a result, authorized modifications to final records must be tracked, and mechanisms must be in place to protect the integrity of data when electronically communicated.

To insure the integrity of information a system-independent mechanism that provides proof against unauthorized modification must be available with each individual object. This integrity proof is on top of other measures taken and applies to all data transmitted over a communications network or in a CE’s possession. Furthermore, the covered entity is required by HIPAA to provide corroboration of the integrity of the data through mechanisms such as checksums, CRCs (Cyclic Redundancy Checks), double keying, message authentication codes or digital signatures. Since this proof against unauthorized modification belongs to an information object while it is transferred between components or systems, if an integrity breach occurs it can be detected.

Users and systems need to be careful about where they send PHI and from where it comes. The issue is to manage data exchanges so they occur only between authorized entities whose identification has been authenticated and who are authorized. This authentication process ensures that rogue data cannot come into a system and masquerade as authentic data.

In messaging systems a strong mechanism for integrity verification is called non-repudiation. It is sufficient to prevent a party from successfully denying the origin, submission or delivery of messages it originates. The technology also protects the integrity of message contents.

3.3 Availability

Patient care is so highly valued there must be a high priority placed on keeping such information available. The health information necessary for patient care needs to be available for access as quickly as possible during normal operations. Furthermore, there must be mechanisms and procedures in place to insure that health information in electronic form continues to be available even in the light of predictable equipment faults or power outages.

For these reasons, and others, health care providers need to plan against disasters. Disasters could include simple machine failures as well as outright destruction of public infrastructure by natural calamities that might wipe out entire installations. The plan against disasters can vary from simple backup tapes, to the use of very comprehensive processes that might include off-site support and backup systems.

4. Security Measures Required by HIPAA

The security requirements outlined in the legislation will lead to complex implementations. In an organization the awareness of security issues has to be supported on all levels. It includes:

- Management involvement in the development and promulgation of HIPAA-compliant security policies and procedures, including periodic review.
- Training on the policies and procedures for all employees that come in contact with PHI during the normal course of their work.
- Technical measures implemented in the organization's information systems, to protect the PHI stored and processed within, or exchanged between them.

The technical measures need to be implemented in such a way that the responsible security manager can trust the implementation. Depending on the type of system, a rigorous proof of confidence may be part of the plan.

The security measures that follow belong to the category of technical measures.

4.1 Authentication

All systems that store, process or protect PHI need to implement access controls in order to manage where this information is allowed to flow and who is allowed to create, view or change it. Authentication follows identification of a user and is accomplished by techniques such as: a secret code only known by a single person, biometrics of a person, a computer readable identity card, or other methods. If the authentication attempt fails then access has to be blocked. All attempts to gain access to a system containing PHI have to be logged for later investigation.

To prevent misuse by other users, if a system is left idle for a period of time, then access to it has to be blocked. Idle time is typically a variable that might be set by the system administrator or the user. When the idle time threshold is crossed the display must be cleared of any patient identifiable data and a new authentication required.

Good policy and procedures are necessary, along with high assurance technology, when implementing identification, authentication, and accountability. For example, if a system can allow a user to print out a report, it might utilize very strong authentication and tracking of the individual

that printed the report. However, an automated system is powerless to track a piece of paper once it has left the printer.

4.2 Authorization

After the authentication process has identified the person accessing the system and authenticated the claimed identity, an authorization mechanism needs to determine what data the user is allowed to access and what functions may be performed. The mechanism can be based on a role a person fulfills in the organization, e.g., administrator, doctor, technician, or on the ownership attribute of data, e.g., medical data of patients of a certain physician.

Authorization is an important security function that hides sensitive information from individuals that have no job-related need to access it. Some individuals may only be allowed to see statistical information; others may have need to access only de-identified medical information, e.g., in a teaching folder. Some individuals may have access to the full set of information about a patient.

Authorization has to be implemented at the lowest level possible to ensure that all access to all PHI is correctly managed. Along with other required security services, such as identification, authentication, and individual accountability, it must be non-bypassable to ensure that all access attempts are controlled and that no one, e.g., system managers, can circumvent it. However, in the case of a crisis, a procedure for emergency override access has to be provided.

4.3 Accountability

All requests for and access granted to stored information must be logged for review and possible investigation. Logging should include such items as a date/time stamp, the identification of the user, the type of access, e.g., create, read, modify, delete, the success or failure of the request, and identification of the data acted upon.

The accountability function must be protected by the system access control mechanism. In this way the system can manage need-to-know and need-to-do of users attempting to access the audit record, and to prevent changes and deletions. It needs to have the same robustness and non-bypassability as other security mechanisms.

Accountability needs to be coupled with specific policies and procedures in order for the data collected in the audit trail to be of any use. The HIPAA privacy regulation requires that successful but unauthorized access to PHI be reported. Without regular inspection of the contents of the audit trail there can be no accountability.

4.4 Integrity Proofing

Many information objects contain cyclic redundancy checks or checksums that indicate if the data has been corrupted while in storage or transit. These methods do not, however, protect against accidental or malicious modification of the data by an otherwise authorized user.

As illustrated in the upper half of Figure 3, a digital signature is a non-refutable proof of integrity and authentication that can be added to information objects. It allows receivers of the object to

verify that the information within it has not been modified and that the information comes from the claimed sender. As a type of checksum, it is calculated from the original object, and encrypted using asymmetric, or private/public key, encryption technology. Any modification after this digital signature is applied will fail the subsequent verification process. Replacing a digital signature is, in practical terms, not possible when the secret key, i.e. the private key of the private/public key pair is unknown to the modifier.

4.5 Secure Transfer

As illustrated in Figure 3, the secure exchange of information objects between two entities requires that a trusted relationship exist between sender and receiver. When the exchange utilizes encryption to provide security the needed trust is linked to the keys used to encrypt and then decrypt the data, and where the keys came from. Note, however, in the HIPAA legislation, encryption is defined as optional for network transmissions within an enterprise or via value added networks or private wire implementations. When the communication lines themselves can't be made secure, e.g., in the case of "open" transmission of data utilizing the Internet or other public network, then encryption might be required.

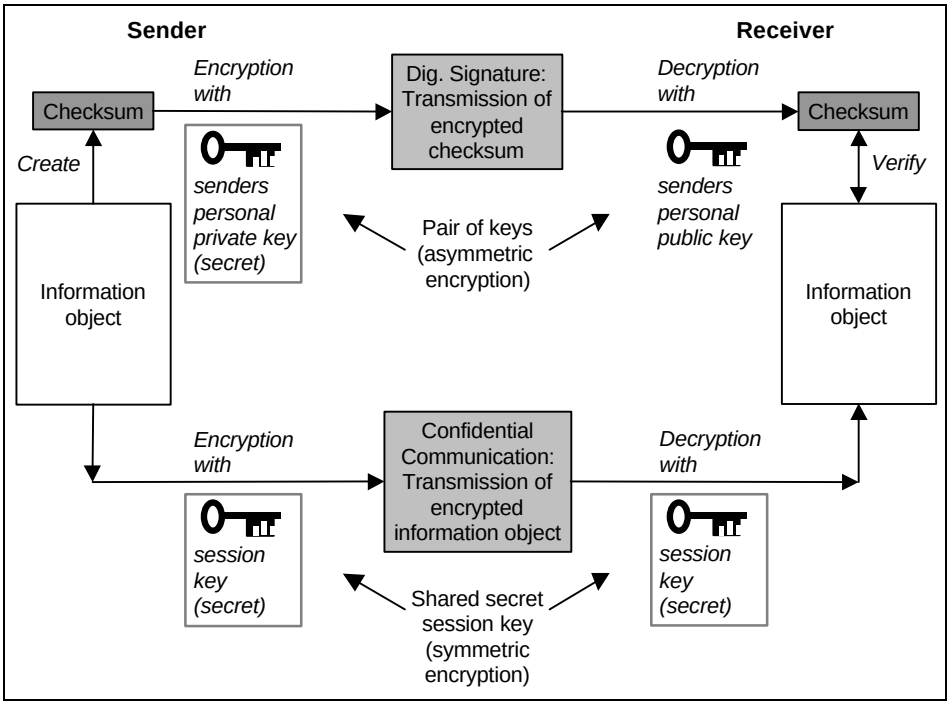

Figure 3: Asymmetric (Private/Public Key) and Symmetric (Shared Secret Session Key) Cryptography Can Facilitate Nonrepudiation, Integrity and Confidentiality Requirements.

During the establishment of a connection for secure data transfer the authentication of both parties has to be verified. Figure 3 shows how a private/public key pair could be used for authentication of the sender. If the authentication succeeds, a shared – but secret – symmetrical session key could be passed for the transfer of the information object in encrypted form, thus safeguarding the data when no secure network is provided between the entities. Using symmetric encryption technology for the actual transfer of data is computationally more efficient, and contributes to timely provision of service.

There are many available protocols that implement this type of secure transfer. Secure Socket Layer (SSL), Transport Layer Security (TLS), and Internet Protocol Security (IPSec), are some of the most common.

4.6 Secure Storage

If PHI is recorded on a media, such as a CD-ROM, and physical transfer of the media is the method used to exchange information, then the same security requirements are applicable. However, in this case since there is no direct connection between the creator system and the reader system, synchronous authentication of the parties and determination of authorization to read the data is not possible. In this case, enforcement of security rules has to rely on the user identification, authentication and authorization technology built into the individual systems the creator uses to store the data on the media, and that the reader uses to access it later.

When the media is not physically protected against unauthorized access, special measures have to be taken to block unauthorized access. For example, if PHI is stored on a CD-ROM and the media is accessible in a public environment, then additional measures are needed to protect the data on the CD-ROM against compromise. The information stored on the media has to be protected using encryption to ensure confidentiality. This could be accomplished using either symmetric or asymmetric encryption. In symmetric encryption, the entities would meet or otherwise securely deliver a symmetric key pair between themselves they would protect against loss, duplication, or unauthorized use. The creator would use this key to encrypt the data onto the media, and the reader would then use its symmetric pair to decrypt the data. This could also be accomplished using asymmetric encryption with the creator encrypting the data onto the media using the intended reader's public key. Then, no one but that reader will be able to decrypt the information using his or her private key.

4.7 Key Management

The use of encryption requires that encryption keys have to be managed inside an organization. Persons who need access to encrypted information require a key with the guarantee that it is the correct key. Safe distribution of keys is a necessary part of security and security administration.

In the case of asymmetric encryption, where private/public key pairs are utilized, a person's private key may only be used on systems with strong authentication mechanisms in place to prevent misuse. The public keys a user maintains must have been distributed in a way that guarantees the key is the authentic public key of the intended communication partner. For this purpose Public Key Infrastructures (PKI) need to be implemented for the purposes of providing certification of the authenticity of one's private and public key pair. The PKI also provides certification of the authenticity of copies of one's public key so it can be relied upon as coming from an authorized source.

Security services using encryption must rely on the proper management of keys and authentication mechanisms. Clear policies and procedures are needed. User training on the potential impacts of key mismanagement, together with effective key management systems, are essential requirements.

5. Privacy Legislations in Other Parts of the World

The European Community has ruled that their members must introduce general privacy laws before the year 2000. This mandate included medical information, which had to be treated with special care. The directive is known as the *EC Data Protection Directive*, EC 95/46. Each country had to develop a specific implementation of the directive, and enact laws assuring compliance with it. In Japan the HPB 517 legislation requires similar security and privacy controls.

These regulations as well as best practices from around the world were considered in preparing this white paper. In reality, healthcare security and privacy is not just a problem specific to the Untied States and to the HIPAA regulations. This is why NEMA is closely cooperating with COCIR, the European Coordination Committee of the Radiological and Electromedical Industry, representing European imaging vendors, and JIRA, representing Japanese imaging vendors, in the definition of globally-effective recommendations on imaging products and their use. In this way we hope to assist healthcare institutions regarding privacy and security regulations.

6. Conclusions

The final HIPAA privacy regulation has now been published and the compliance date for many health care providers is February 26, 2003. Once the final security regulation is published there will be approximately 26 months before it becomes effective.

While specific enforcement procedures are not well defined at this time, there are penalties built into the regulations for those who do not comply. It is not clear whether the United States Government will conduct inspections or require certifications, but they will likely react to incidents where the privacy of PHI has been compromised. In this scenario an investigation of the policy and procedures available at and enforced within a CE is likely. If negligence is found, fines could be levied. In addition accreditation organizations, e.g. JCAHO and NCQA, have indicated that they will integrate privacy and security requirements based on HIPAA.

A compelling motivation for CEs to enact strict HIPAA-compliant security and privacy policies and procedures, and for vendors to ensure they provide technology solutions that can contribute to HIPAA compliance is the legal community. It can be anticipated that HIPAA-related privacy violation cases against healthcare organizations, insurance companies and business associates will be vigorously litigated.

All of these factors build a strong case to remain informed and begin today to identify security and privacy compliance solutions that can benefit health care organizations and the health imaging industry.