From: Hornberger, Zack <ZHornberger@medicalimaging.org>
Sent: Thursday, October 24, 2019 9:16 AM
To: privacyframework <privacyframework@nist.gov>
Subject: RE: Preliminary Draft of the Privacy Framework

Dear Ms. MacFarland:

As the leading trade association representing the manufacturers of medical imaging equipment and radiopharmaceuticals, the Medical Imaging & Technology Alliance (MITA) commends the National Institute of Standards and Technology (NIST) for its continued work to improve and facilitate manufacturing practices amongst business owners, software developers, and cybersecurity professionals that promote the privacy of digital information. MITA is a strong supporter of efforts that improve the privacy and security of our ever-increasing digital infrastructure, and we believe that this document will help organizations better integrate privacy risk management into their overall risk management and cybersecurity programs. The attached comments are provided to strengthen that aim.

If you have any questions, please let me know.

Sincerely,

Zack Hornberger

Director of Cybersecurity & Informatics

Medical Imaging & Technology Alliance (MITA), A Division of NEMA

1300 North 17th Street, Suite 900 Arlington, VA 22209

Phone: 703.841.3285

zhornberger@medicalimaging.org

MITA MEMBER WORKSPACES

XRAY Section & Workgroups | Cybersecurity Committee | Medical Imaging Informatics Section | Artificial Intelligence

MITA®
MEDICAL IMAGING
& TECHNOLOGY ALLIANCE
A DIVISION OF NEMA®

1300 North 17th Street ▪ Suite 900
Arlington, Virginia 22209
Tel: 703.841.3200
Fax: 703.841.3392
www.medicalimaging.org

October 24, 2019

Katie MacFarland
National Institute of Standards and Technology
Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899

Via email: privacyframework@nist.gov

RE: Preliminary Draft of the Privacy Framework

Dear Ms. MacFarland:

As the leading trade association representing the manufacturers of medical imaging equipment and radiopharmaceuticals, the Medical Imaging & Technology Alliance (MITA) commends the National Institute of Standards and Technology (NIST) for its continued work to improve and facilitate manufacturing practices amongst business owners, software developers, and cybersecurity professionals that promote the privacy of digital information. MITA is a strong supporter of efforts that improve the privacy and security of our ever-increasing digital infrastructure, and we believe that this document will help organizations better integrate privacy risk management into their overall risk management and cybersecurity programs. The following comments are provided to strengthen that aim.

MITA supports the framework's emphasis on the misconception of a "one size fits all" approach. Such approaches are often compliance-oriented and have become more common in the absence of a more thorough understanding of how to practice risk management.

The section on Privacy Risk (1.2.1) describes the experience of a breach as a form of harm, either tangible or intangible. However, since most individuals affected by a typical data breach do not experience a direct harm from a data breach (as demonstrated by the difficulty in assessing damages resulting from a data breach), it is more appropriate to think of privacy in terms of privacy principles, and a privacy risk defined in terms of the potential to violate a privacy principle. The more restricted realm of adverse events that result in some form of harm is not appropriate for privacy. Most privacy frameworks are based on privacy principles, such as protecting against data disclosures, or allowing individuals to exercise control over data.

The Venn diagram in the section depicts the intersection of "cybersecurity risk" and "privacy risk" as "data breach". A "data breach" is only one type of adverse event associated with these risks. It is not the appropriate name for the complete area of intersection. In fact, a "data breach" can occur outside the digital space and this would not be within the area of intersection. In a recent case involving a Canadian organization, the organization was found to have sent private data on paper records to a landfill. A more accurate example of the intersection area would be "Breach of digitized private data".

The combination of threat-based risk management and the application of privacy principles is an important element of privacy risk management. While the concept of a security risk is generally threat-based, a privacy event can occur in the absence of an identified threat. We encourage NIST to consider this dichotomy during the revision of the draft.

Section 1.2.2 addresses Privacy risk management as a component of risk management. The list of approaches (starting on line 258) provides a good initial framework to risk management. However, approaches could be clarified by differentiating mitigations (that reduce impact of any potential privacy adverse event), remediations (that reduce the likelihood of an adverse event occurring), and so on.

The concept of "risk transfer" (via contract, for example) is an important element to consider. This does not reduce the risk of an event in any way, but rather is focused on reducing liability to an organization which is important to emphasize.

It would be useful to introduce the concept of the "Privacy Impact Assessment (PIA) in section 2.1. This is a process by which an organization can identify privacy risk impact of specific business activities or products, identify opportunities for mitigations, and provide the basis for determining required controls. A PIA can be used to better manage design of business activities or products as an evaluation tool.

"Accountability," identified in section 3.2, is labelled a privacy principle. It would be better labeled as a privacy risk-management principle.

In section 3.6 we note that if an organization's products or services have privacy risk impact (e.g. MedTech), then the organization can apply many privacy risk management practices to its products and services to enable privacy risk management by its customers. The organization must consider the intended and/or expected uses of its products, and the use environment, to better collaborate with customers on risk management.

MITA counts on your careful consideration of these comments, and we look forward to working with NIST in the completion of this important effort.

If you have any questions, please contact Zack Hornberger, Director of Cybersecurity & Informatics, at zhornberger@medicalimaging.org or (703) 841-3285.

Sincerely,

Patrick Hope
Executive Director, MITA

MITA is the collective voice of medical imaging equipment and radiopharmaceutical manufacturers, innovators and product developers. It represents companies whose sales comprise more than 90 percent of the global market for medical imaging technology. These technologies include: magnetic resonance imaging (MRI), medical X-Ray equipment, computed tomography (CT) scanners, ultrasound, nuclear imaging, radiopharmaceuticals, radiation therapy equipment, and imaging information systems. Advancements in medical imaging are transforming health care through earlier disease detection, less invasive procedures and more effective treatments. The industry is extremely important to American healthcare and noted for its continual drive for innovation, fast-as-possible product introduction cycles, complex technologies, and multifaceted supply chains. Individually and collectively, these attributes result in unique concerns as the industry strives toward the goal of providing patients with the safest, most advanced medical imaging currently available.