Dr. Walter G. Copan

Director

National Institute of Standards and Technology

100 Bureau Drive, Stop 2000

Gaithersburg, MD 20899

Dear Dr. Copan:

Introduction:

Thank you for allowing us the opportunity to comment on the Privacy Framework. Maize Analytics is a software development company that leverages machine-learning, advanced understanding of clinical workflows, and statistical ranking to audit accesses to a patient's electronic medical record (EMR). Maize Analytics believes protecting a patient's electronic protected health information (ePHI) contained in the EMR is a significant challenge for all healthcare organizations operating today. The use of artificial intelligence (AI) and machine learning greatly enhances a healthcare organization's ability to audit EMR accesses for privacy violations. However, the use of AI should not be adopted without first carefully evaluating the technology against fundamental privacy principles and HIPAA requirements.

The Privacy Framework should provide the tools necessary for privacy officers and healthcare organizations to effectively evaluate technology that assists in protecting privacy. Maize believes that general principles stated in HIPAA regulations, the fair information practice principles (FIPPs), and the three privacy engineering objectives of predictability, manageability, and disassociability provide excellent guidance on how the Privacy Framework can enable privacy professionals to assess emerging technologies. When evaluating emerging technologies, the Privacy Framework should encourage privacy professionals to answer two questions. Does the privacy technology analyze the data action, the ePHI involved, and the context of the problematic data action? Does the technology operate with sufficient transparency to explain how the technology enhances the organization's ability to meet privacy engineer objectives, FIPPs goals, and HIPAA requirements?

HIPAA Auditing Standard:

HIPAA regulations require covered entities to "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[1] Additionally, a covered entity is required to have audit controls in place to examine activity in electronic systems that contain ePHI. A healthcare organization is required to "[i]mplement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."[2] The HIPAA security rule adopts a flexible approach, "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 specifications as specified in this subpart."[3] When a covered entity is deciding what security measures to use to comply with the HIPAA security rule, it must account for the following factors: "(i) The size, complexity, and capabilities of the covered entity . . . [;] (ii) The covered entity's . . . technical infrastructure, hardware, and software security capabilities[;] (iii) The costs of security measures [;] (iv) The probability and criticality of potential risks to electronic protected health information."[4] A covered entity is required to implement a reasonable EMR audit process given the unique risks to ePHI at the covered entity and the resources available to the organization.

In January 2017, the HHS OCR published a Cybersecurity Newsletter on the importance of audit controls required under the HIPAA Security Rule. The newsletter identified four points that healthcare organizations should consider. (1) What audit control mechanisms are reasonable and appropriate to implement so as to record and examine activity in information systems that contain or use ePHI? (2) What are the audit control capabilities of information systems with ePHI? (3) Do the audit

controls implemented allow the organization to adhere to their audit control policies and procedures? (4) Are changes or upgrades of an information system's audit capabilities necessary?[5]

Healthcare organizations have an incentive to provide healthcare providers broad access to the EMR to ensure the providers have the information necessary properly treat patients. The HIPAA privacy rule only permits the use and disclosure of a patient's ePHI for treatment, payment, or health care operations.[6] However, the accessibility of the EMR by the workforce provides opportunities for privacy violations by individuals who are authorized to access the EMR; therefore, the broad access health care providers have to a patient's EMR poses a risk that a patient's PHI could be accessed by an employee of a healthcare organization with access rights but no justification under the HIPAA privacy rule. Auditing of the EMR system is necessary to identify employees who do not have the authorization to access a patient's medical records. An effective audit program coupled with appropriate discipline and training should produce a deterrent effect for unauthorized accesses in the context described above. The Privacy Framework must enable healthcare organization to evaluate technology against required auditing and privacy standards.

Privacy Principles:

The effectiveness of technology-assisted audits should be evaluated against the software's ability to assist the privacy office in operationalizing the fair information practice principles. The FIPPs include access and amendment, accountability, authority, minimization, quality and integrity, individual participation, purpose specification and use limitation, security, and transparency.[7] Additionally, the emerging field of privacy engineering establishes basic principles and objectives that can be used to assist in the evaluation of how software is used to address privacy risk. The principles of privacy engineering lie at the intersection of information systems and privacy. NIST Internal Report 8062 describes the three objectives of privacy engineering – predictability, manageability, and disassociability.[8] The privacy engineering objectives align with the FIPPs.

NIST Internal Report 8062 comments on the FIPPs, stating that the FIPPs "have enduring value by articulating expectation regarding appropriate information practices, and they have helped many organizations to develop baseline considerations for protecting individual's privacy as new technologies enter the marketplace." [9] However, the FIPPs have limitations regarding their ability to analyze privacy risk and contribute to the development of a repeatable and measurable process.[10] "[P]ut another way, evaluating how the FIPPs should be applied, particularly across different types of systems, without an independent frame of reference, provides no point of comparison."[11] If privacy risks are not properly modeled in the terms scope, vulnerabilities, likelihood and severity, the privacy risk analysis would be completely ad hoc and idiosyncratic as it relates to the institution or personnel conducting the risk assessment.[12] The Privacy Framework should provide a process for privacy officers and institutions to evaluate privacy technology that is both measurable and repeatable. Maize believes the Privacy Framework should adopt an evaluation process that is consistent with the risk model discussed in NISTIR 8062 to ensure technology utilized by a privacy office is objectively reviewable and consistent with the organization's enterprise risk management program. The privacy risk model must frame the evaluation.

Privacy Risk and Risk Model:

The primary risk to EMR privacy is unauthorized access of ePHI by a workforce member. Technology can assist privacy officers in identifying the unauthorized accesses; however, the adoption of technology is not without risk. When adopting AI technology to help in EMR auditing, a healthcare organization risks that the technology will fail to properly audit the records and lack the transparency to show how the technology conducts audits. Privacy offices must have clear objectives and a firm understanding of how the technology works to ensure their adoption of the technology is defensible if they are required to justify their adoption of the technology to regulatory agencies.

The common information security terms "threat" and "vulnerability" fail to adequately articulate the nature of privacy risks because many privacy risks arise from "authorized" behaviors.[13] If information security principles are applied to privacy problems, the information security principles may fail to identify threats because some activity may be authorized as it relates to information security but unauthorized as it relates to privacy concerns. The unauthorized access of patient data in an EMR is a prime example of the divergence of information security and privacy. The NIST privacy engineering model uses the term "problematic data-action" rather than attempting to expand the "threat" risk factor to encompass pure privacy concerns.[14]

"Problematic data action means a data action that causes an adverse effect, or problem, for individuals."[15] Maize believes that the Privacy Framework should adopt the concept of the "problematic data-action" as described in NISTIR 8062.

The problematic data action in the privacy risk model frames the issue in the same way that threats define adverse events in the information security risk model.[16] After a problematic data action has been identified, the assessment continues by addressing likelihood and impact.[17] Three key characteristics of problematic data actions can assist in determining the likelihood and impact: data action, personally identifiable information (PII or ePHI in the context of EMR), and context.[18]

A data action is any discrete system operation that processes PII.[19] A risk assessment should work to determine what data actions could be problematic. In the context of EMR access, the lack of traditional security controls due to patient care optimization significantly increase the likelihood of a problematic data-action by a workforce member. PII is information that can be used to distinguish or trace a person's identity.[20] In the EMR context, HIPAA clearly defines ePHI and what information the healthcare organization must protect. The impact of unauthorized access and disclosure of ePHI can be grouped into three general categories: legal and regulatory costs; reputation costs leading to loss of trust and revenue; and failure for patients to be willing to adopt systems using ePHI and lose the benefits of improved healthcare.[21] Additionally, ePHI containing information regarding sexually transmitted disease or mental health records pose a significant risk of embarrassment to the patient. A patient could also suffer a substantial risk of financial harm or discrimination if an employer or insurance company gains unauthorized access to the EMR. The final characteristic, context, is defined as the circumstances surrounding the system's processing of PII.[22] The context of the data action provides the boundary where action becomes problematic. For example, clerical staff in a hospital do not need to access a patient's entire medical record to admit a patient; however, a treating physician would need access to the patient's whole medical history to ensure appropriate treatment. The context of the encounter matters with regard to the information accessed by a workforce member. Maize believes the context of the data action is the most critical factor in determining whether an EMR access is appropriate or suspicious.

The technology and process used by privacy officers lead to the identification of problematic data actions by assessing the data actions, identifying the ePHI accessed, and providing the necessary context to determine the appropriate boundary. The Privacy Framework should require technology assisting privacy compliance to clearly identify the data action, the information accesses or disclosure, and the context of the particular data action in a transparent manner that ensures privacy officers and organizations can understand how the technology works.

Transparency of Technology:

The openness of algorithms used to assist with EMR audits is key to justifying the use of AI to audit EMR records. If the technology is not transparent, the privacy officers run the risk of relying on a flawed system to audit EMR accesses. The Harvard Business Review recently published an article outlining the need to audit algorithms.[23] The authors argue that society may be overlooking some problems with introducing algorithms into business and relying on the notion that large datasets can yield reliable and objective truths if mined by machine learning tools.[24] "It is by now abundantly clear that, left unchecked, AI algorithms embedded in digital and social technologies can encode societal biases, accelerate the spread of rumors and disinformation, amplify echo chambers of public opinion, hijack our attention, and even impair our mental wellbeing."[25] The authors argue that establishing a discipline of algorithm auditing is a necessary part in addressing the challenges of AI governance, auditing, risk management, and control.[26]

Additionally, the FDA is currently developing a software precertification program to evaluate and certify software that functions as a medical device.[27] The goals of the program are to establish trust, leverage transparency, and verify effectiveness and performance in the real world.[28] Software utilized to protect privacy should also be tested against similar principles to ensure the technology performs as promised.

Conclusion:

Due to requirements imposed by HIPAA, healthcare organizations must demonstrate they are taking reasonable steps to audit the EMR for privacy compliance. The first step to effectively leverage technology to aid privacy compliance is the objective evaluation of the technology being considered by the organization. The Privacy Framework should provide a method

for organizations to evaluate technology against identified privacy risks and demonstrate the efficacy of the technology. The Privacy Framework should evaluate privacy technology by assessing how well the technology evaluates the three characteristics of problematic data actions – data action, PII, and context. Privacy technology must be transparent and enable organizations to articulate how the technology arrived at its assessments or conclusions by providing human readable text descriptions and details showing what evidence was used to make decisions. Transparency will allow organizations utilizing technology to aid in privacy audits to demonstrate how the implementation of technology relates back to privacy engineering objectives and the FIPPs.

Sincerely,

Daniel Fabbri, PhD
CEO, Maize Analytics

References:

[1] 45 C.F.R. § 164.308(a)(1)(ii)(D) (2018).
[2] 45 C.F.R. § 164.312(2)(d) (2018).
[3] 45 C.F.R. § 164.306(b)(1) (2018).
[4] 45 C.F.R. § 164.306(b)(2) (2018).
[5] U.S. DEP'T. OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, UNDERSTANDING THE IMPORTANCE OF AUDIT CONTROLS (Jan. 2017), https://www.hhs.gov/sites/default/files/january-2017-cyber-newsletter.pdf.
[6] 45 C.F.R. § 164.506(a) (2018).
[7] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH, NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS app. f (Jan. 2017), https://doi.org/10.6028/NIST.IR.8062 [heterinafter *NISTIR 8062*].
[8] *Id. at 17.* The principles of privacy engineering are not intended to replace the FIPPs. They are designed to supplement the FIPPs and increase the level of precision when controls are selected to address privacy risks. In the case of EMR access by internal employees, audit controls are the best available controls because the control does not interfere with patient care or increase risk to patient safety.
[9] *Id.* at 11.
[10] *Id.*
[11] *Id.* (*citing* STUART S. SHAPIRO, HOMELAND SEC. SYS. ENG'G & DEV. INST., SITUATING ANONYMIZATION WITHIN A PRIVACY RISK MODEL 2 (2012), https://www.mitre.org/sites/default/files/pdf/12_0353.pdf.)
[12] SHAPIRO, *supra* note *11,* at 1.
[13] NISTIR 8062 *supra* note 7, at 21.
[14] *Id*.
[15] *Id*.
[16] *Id*.
[17] *Id*.
[18] *Id*. at 22.
[19] *Id*. at 23.
[20] *Id*.
[21] *Id*. at 22.
[22] *Id.*
[23] James Guszcza et. al., *Why We need to Audit Algorithms,* Harvard Business Review (Nov. 28, 2018), https://hbr.org/2018/11/why-we-need-to-audit-algorithms.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] U.S. DEP'T. OF HEALTH & HUMAN SERVS., U.S. FOOD AND DRUG ADMINISTRATION, DEVELOPING A SOFTWARE PRECERTIFICATION PROGRAM: A WORKING MODEL V.1.0 (Jan. 2019), https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/UCM629276.pdf.
[28] *Id.* at 6.