## Privacy and Security Workgroup (PSWG)

# Meaningful Use (MU) Stage 3 Notice of Proposed Rulemaking (NPRM) Objective 1: Protect Patient Health Information

**Comment on the proposed addition of administrative and technical safeguards to protect patient information created or maintained by Certified Electronic Health Record Technologies (CEHRT).**

| **Medicare and Medicaid Programs; Electronic Health Record Incentive Program – Stage 3<br>Objective 1: Protect Patient Health Information – Request for Comment** |
|---|
| pp. 16746 - 16747of FR Vol. 80, No. 60: … we are proposing to maintain the previously finalized Stage 2 objective on protecting ePHI. However, we propose further explanation of the security risk analysis timing and review requirements for the purposes of meeting this objective and associated measure for Stage 3. . . .<br><br>(Proposed Objective): Protect electronic protected health information (ePHI) created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical, administrative, and physical safeguards.<br><br>(Proposed Measure): Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (including encryption) of data stored in CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the provider's risk management process. (Continued on p. 16747 and p. 16798) |
| |

**Public Comment Field:**

The Workgroup supports the proposed MU Stage 3 security requirements. By adding administrative and physical safeguards to the current requirements, Certified Electronic Health Record Technology (CEHRT) risk assessments and attestations are now more closely aligned with the compliance requirements of the HIPAA Security Rule.

# Privacy and Security Issues Related to Increasing Patient Access to Data (e.g., via view, download, and transmit (VDT) and application programming interfaces (APIs))

**Comment on the privacy and security issues related to increasing patient access to health data via view, download, and transmit (VDT) technologies and application programming interfaces (APIs).**

| **Medicare and Medicaid Programs; Electronic Health Record Incentive Program – Privacy and Security Issues Related to Increasing Patient Access to Data (i.e., VDT, APIs)**<br>**Generally related to Objective 5 (Patient Electronic Access to Health Information)** |
|---|
| p. 16752: The Stage 1 and Stage 2 final rules included a number of objectives focused on increasing patient access to health information and supporting provider and patient communication . . . . For Stage 3, we generally identified two related policy goals within the overall larger goal of improved patient access to health information and patient-centered communication. The first is to ensure patients have timely access to their full health record and related important health information; and the second is to engage in patient-centered communication for care planning and care coordination. While these two goals are intricately linked, we see them as two distinct priorities requiring different foci and measures of success. For the first goal, we are proposing to incorporate the Stage 2 objectives related to providing patients with access to health information, including the objective for providing access for patients (or their authorized representatives) to view online, download, and transmit their health information and the objective for patient-specific education resources, into a new Stage 3 objective entitled, "Patient Electronic Access" (Objective 5), focused on using certified EHR technology to support increasing patient access to important health information. For the second goal, we are proposing an objective entitled Coordination of Care through Patient Engagement (Objective 6) incorporating the policy goals of the Stage 2 objectives related to secure messaging, patient reminders, and the ability for patients (or their authorized representatives) to view online, download, and transmit their health information using the functionality of the certified EHR technology. . . .<br><br>p. 16753: We are also proposing to expand the options through which providers may engage with patients under the EHR Incentive Programs. Specifically, we are proposing an additional functionality, known as application-program interfaces (APIs), which would allow providers to enable new functionalities to support data access and patient exchange.<br><br>(Continued on pages 16754-16755, 16799) |
| |

**Public Comment Field:**

Generally, the **Workgroup supports the proposal to increase the opportunities for patient access to information through the use of both "view/download/transmit" (VDT) as well as open application programming interfaces (APIs)**, as this advances the fair information practice principles of individual access and openness and transparency.

However, the Workgroup remains concerned about potential privacy and security risks associated with increasing patient access to health information electronically via APIs or VDT technologies. These include risks patients may face when taking control of this information or having it sent directly to others (or that patient authorization may be spoofed by companies seeking unauthorized access to data), as well as some risks providers may face, such as security risks from connecting to patient devices or apps.

The Workgroup first recommends that ONC and CMS **reference and leverage**, where appropriate, previous Health IT Policy Committee **recommendations (which came from the Privacy and Security Tiger Team (PSTT)) regarding best practices for view and download**. These best practices are captured in the Health IT Policy Committee transmittal letter

of August 16, 2011. (Available at: http://www.healthit.gov/sites/faca/files/HITPC_PSTT_Transmit_8162011.pdf **Although these best practices were developed in the context of view and download, they are equally applicable to "transmit" and the use of APIs to capture data.** To the best of our knowledge, these recommendations have yet to be acted on as part of the MU and certification programs. The Workgroup recommends that the **guidance is updated to address transmit-related risks and issued in a timely fashion to assist providers (and CEHRT vendors) in making VDT and APIs available to patients as part of MU.** Such guidance should address issues that include the following: when liability for data shifts from providers to patients, and the extent to which providers must make patients aware when patients take responsibility for protecting data; best practices for counseling patients on assessing and managing privacy and security risks; responsibilities for vendors to include CEHRT security safeguards in VDT and API modules; technical approaches vendors may take to further protect data (for example, "just in time" notices before download and transmit that should be able to be turned off by the patient after the first notice, and non-caching of data).

Second, **ONC should continue its work with FTC and OCR to develop guidance for key stakeholders as more patients, providers, and researchers adopt the use of mobile IT, software applications (apps), and APIs**. The Workgroup **urges the agencies to work quickly to disseminate this guidance so it can be useful for Stages 2 and 3 of MU**. Specifically, private industry app developers would greatly benefit from guidance about privacy and security best practices related to the collection, storage, access, use, transmission, and destruction of health information, and methods for clearly communicating their privacy policy and security practices to patients and providers. The Workgroup also agrees that the guidance would be beneficial for the app developers who may not be covered by HIPAA but whose products are intended to capture data, on behalf of patients or their authorized representatives, from entities covered by HIPAA. In addition patients and providers would benefit from guidance on the safe use of apps and APIs, which could include a checklist for patients to consider when choosing apps and what to look for in a privacy/data use policy. Workgroup members suggest that **ONC and OCR produce guidance and educational materials for both patients and providers on the safe use of apps and APIs.** Such guidance could provide patients with information about customary practices, common security risks, and guidance on how to find, compare and evaluate an app's privacy policy and terms of service. ONC's Personal Health Record (PHR) Model of Privacy Notice can be leveraged as a model for developing such guidance. Guidance to providers should focus on evaluating and managing potential security risks of APIs and how to advise patients on evaluating apps and making wise choices. ONC and OCR should widely disseminate such guidance to maximize its efficacy.

Third, the Workgroup wishes to reinforce its prior recommendations on **identity proofing and authentication of patients** seeking to access information in a provider EHR as part of meaningful use and its recommendations on enabling patients to provide access to friends and family members.

Fourth, the Workgroup suggests that **ONC and OCR issue guidance addressing the intersection between the meaningful use patient engagement objectives, the certification requirements, and HIPAA's patient access rights**. The guidance could also be used to help providers in Stages 2 and 3 of the Meaningful Use program. Specific issues to address should include: how to conduct a security risk assessment on patient app/device connections (such as through the API) and the extent to which a provider may reject a patient's request for electronic access due to a perceived security risk for the provider; the extent to which a provider may reject a patient's request for electronic access in the absence of a security risk; and the ability of providers to charge fees for meaningful use access in circumstances where the patient is requesting HIPAA access through use of the certified EHR functionalities.

Finally, the Workgroup calls for further exploration of **a multi-stakeholder (including industry and patients) developed program to evaluate patient-facing health apps**. The Workgroup believes the apps should be evaluated on a range of aspects, including privacy and security, usability for consumers/patients, and clinical validity. The program should leverage the guidance developed by federal government entities (see above). Such a program could not only help patients choose the apps that best meet their needs and address their particular privacy concerns, but also help providers counsel their patients and evaluate potential security risks to their EHR systems. Even guidelines that are adopted voluntarily could be enforced by the FTC under its existing FTCA authority. The Workgroup also proposes that the **Consumer Workgroup (with assistance from the Privacy and Security Workgroup) continue work to flesh out the details of an evaluation program**. Issues to be considered include the following: whether the program should be a

certification program, which includes testing (similar to the CEHRT program) or some other evaluation vehicle (e.g., accreditation, registry, etc.); whether the program should be voluntary or connected to the CEHRT and/or MU; potential incentives/disincentives for vendors to participate in the program; the focus of the program; the role of ONC and other federal entities; and the cost and potential impact on innovation.