PSTT04: What, if any, security risk issues (or Health Insurance Portability and Accountability Act (HIPAA) Security Rule provisions) should be subject to Meaningful Use attestation in Stage 3?

*[For example, the requirement to make staff/workforce aware of the HIPAA Security Rule and to train them on Security Rule provisions is one of the top 5 areas of Security Rule noncompliance identified by the HHS Office for Civil Rights over the past 5 years.  In addition, entities covered by the Security Rule must also send periodic security reminders to staff. The HITPC is considering requiring EPs/EHs/CAHs to attest to implementing HIPAA Security Rule provisions regarding workforce/staff outreach & training and sending periodic security reminders; we seek feedback on this proposal.]*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Comment ID | PSTT04 | Name of Respondent | Organization | Summary of Comments |
| 1 | [HHS-OS-2012-0007-0534](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0534) | #2/p.2-3 | Samantha  Halpert | Federation of American Hospitals | * Deferred to the Confidentiality Coalition for comments regarding privacy and security. * See Comment #24, Confidentiality Coalition. |
| 2 | [HHS-OS-2012-0007-0388](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0388) | p. 1 |  | Crowe Horwath LLP | * Stated that HIPAA Security Rule awareness and training for staff/workforce is appropriate. * Suggested adding in a revision to ensure all workforce members are also trained on security awareness and are informed of the various facets of phishing attempts as part of the HIPAA Security Rule training is appropriate. * Stated employees/workforce should be trained on how to identify and respond to security incidents, including the person(s) in the organization who should be contacted. * Suggested that the following are logical next steps for inclusion in Meaning Use (MU) Stage 3: * Ensuring all EPs/EHs/CAHs implement data backup plans for all EHR/EHR modules. The data backup plans should also include retention of records per state and federal regulations. * Ensuring all EPs/EHs/CAHs employee/workforce members’ workstations accessing EHRs/EHR modules are running antivirus/malware/spyware, firewall and/or HIPS and are part of the entity’s patch management solution to ensure these endpoint devices are protected from malicious content. * Ensuring all EPs/EHs/CAHs employee/workforce members’ laptop/mobile devices accessing EHR/EHR modules include full-disk encryption to protect against the loss of data in the event of a theft or loss of device. |
| 3 | [HHS-OS-2012-0007-0397](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0397) | p. 12 | Alice Borrelli | Intel Corporation | * Commented that social media and mobile devices, including trends such as Bring Your Own Device (BYOD) empower healthcare workers. * Stated that social media and mobile devices (including BOYD) present significant privacy and security risks, such as: * Confidentiality of PHI as it moves through unsecured channels, for example unencrypted patient information exchanged through file transfer applications or texted between healthcare providers. * Integrity (completeness) of patient information as the exchange of healthcare information out-of-band with the EHR through workarounds like this generally does not result in updates to the patient record, causing the patient record to become incomplete. * Suggested security solutions must be usable to avoid use of alternatives and workarounds, which can bring additional risk. * Stated that hardware assisted security plays a key role in improving the usability in healthcare security solutions, for example hardware accelerated encryption. * Suggested that healthcare organizations implement effective administrative security controls including policy, procedures, risk assessment, and training, with key emphasis placed on effective training. * Stated that training needs to go beyond traditional “once-a-year” security awareness training, and provide timely, well targeted security training to healthcare workers when they need it. For example, if a healthcare worker tries to copy unencrypted healthcare information to a USB stick, out of compliance with the healthcare policy, a DLP solution should alert and provide training to the healthcare worker to avoid a breach and recurrence. |
| 4 | [HHS-OS-2012-0007-0425](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0425) | p. 14 | Willa Fields, Stephen Lieber | HIMSS | * Agreed that the “human element” – employee security awareness and organizational culture are important indicators of an entity’s ability to protect information. * Suggested requiring attestation for awareness as part of the environment, training, and sanctions. * Recommended requiring that data stored on removable media be encrypted when outside protected environments. * Recommended that portable devices (laptops) have full-disc encryption. * Recommended policies and procedures to prohibit local storage of PHI. * Suggested that if such storage is important for specific users or the clinical workflow in any regard, then security controls (technical, administrative and physical) should be identified so that the risk to PHI is adequately mitigated. |
| 5 | [HHS-OS-2012-0007-0412](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0412) | p. 14 | John Travis | Cerner Corp. | * Suggested that any security certification criteria clearly delineate responsibility between the EHR software platform and the user (hospital or eligible provider), including expected policy and procedures, training programs and sanction programs for the institution. |
| 6 | [HHS-OS-2012-0007-0409](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0409) | p. 18 | William Zoghbi | American College of Cardiology | * Recognized that ensuring that patient health information is protected and secure is important. * Supported efforts by the government to include relevant objectives and criteria as part of the federal EHR Incentive Program. * Does not believe that collecting attestations regarding the implementation of HIPAA Security Rule provisions is a worthwhile exercise. * Stated that penalties of the HIPAA Security Rule for a covered entity found in violation of the Security Rule and Privacy Rule is sufficient. * Stated that attestation is redundant and unproductive. * Urged the HITPC to withdraw the proposal. |
| 7 | [HHS-OS-2012-0007-0376](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0376) | p. 19 | Sarah Cottingham | Telligen Iowa HIT Regional Extension Center | * Suggested assignment and training on the roles of the HIPAA Security Officer. |
| 8 | [HHS-OS-2012-0007-0431](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0431) | p. 20 | Susan Turney | Medical Group Management | * Does not believe it is appropriate to include any additional security steps as a component of meaningful use Stage 3 attestation. * Stated application of HIPAA Security Rule’s requirements for risk assessment and mitigation of any identified risks is adequate. * Requiring an EP to conduct another security risk analysis is duplicative, adding an unnecessary reporting burden. * Remarked that while encryption is a laudable goal, it is an addressable requirement under the Security Rule. It is not required. * Encouraged CMS to work with the Office for Civil Rights (OCR) in development of guidance and educational materials to assist physician practices understand and implement encryption for circumstances in which the covered entity determines encryption is an appropriate solution. * Commented that HIPAA Security regulation outlines the process a covered entity must go through for completing a risk assessment, but does specify the exact steps, milestones and outcomes of that analysis. * Commented that compliance with the risk assessment requirements of the HIPAA Security Rule and fulfillment of this meaningful use objective has proven very difficult, especially for smaller practices that have limited in-house expertise in this area. * Encouraged CMS to work with the OCR to develop guidance and education on the issue of risk assessment and risk mitigation. |
| 9 | [HHS-OS-2012-0007-0395](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0395) | p. 28 | Paula Bussard | The Hospital & Health System Association of Pennsylvania | * Stated that training on the Security Rule and sending of security reminders are important. * Stated that the Meaningful Use rule should not be used as a means to enforce compliance with all HIPAA privacy and security requirements, including those for making staff and workforce members aware of the HIPAA Security Rule and to train them on Security Rule provisions. * Believed that meaningful use attestation about implementing the HIPAA rules is unnecessary. * Stated that reliance on Meaningful Use requirements to require implementation of HIPAA Security and Privacy may lead to a potentially different or conflicting set of compliance obligations enforced by multiple agencies through multiple and uncoordinated means. * Urged rejection of requirements for EPs/EHs/CAHs to attest to implementing HIPAA Security Rule provisions regarding workforce/staff outreach and training and sending periodic security reminders. |
| 10 | [HHS-OS-2012-0007-0382](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0382) | p. 34 | Cheryl Peterson/Karen Daley/Marla Weston | American Nurses Association | * Stated that OCR already requires considerable input from providers to meet HIPAA requirements. * Commented that requiring additional attestation from providers to meet ONC criteria will cause undue burden and exceed the ONC charter. |
| 11 | [HHS-OS-2012-0007-0391](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0391) | p. 4 | Karen Boykin-Towns | Pzfizer Inc | * Supported the HITPC’s recommendation that EHRs be able to accept two factor or higher authentication for provider users to remotely access protected health information (PHI) in Stage 3. * Noted that the Drug Enforcement Administration (DEA) requires two factor authentication for any provider who wants to send controlled substances electronically. * Suggested that EHR capabilities should include DEA authentication requirements for prescribers. |
| 12 | [HHS-OS-2012-0007-0429](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0429) | p. 7 | Deven McGraw | Center for Democracy and Technology | * Noted that the HHS Office for Civil Rights (OCR) increased enforcement of the HIPAA regulations and the audits can reveal important information on the most common security issues that are not adequately addressed by covered entities and business associates. * Suggested that HITPC, ONC and CMS can advise on these commonly neglected Security Rule provisions. * Stated that these commonly neglected Security Rule provisions should be included in Stage 3 Meaningful Use attestation. |
| 13 | [HHS-OS-2012-0007-0525](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0525) | p.1 | David Finn | Symantec Corp. | * Commented that there was no doubt that security and privacy risks are “people problems”. * Stated that employee awareness and the organization’s culture may be the best indicators of an organization’s ability protect information. * Suggested attestation should focus on three primary areas: 1) workplace awareness (posters, reminders, etc.); 2) workforce, BAs and contractors training (on-going, not once/year), and; 3) workforce, BAs and contractors sanctions (real sanctions, enforced consistently, regardless of role or function). * Commented that breaches over the past 3 years evidence that a sizable majority are related to portable devices (laptops, tablets, smartphones) or removable media (tapes, jump drives, removable disks). * Suggested that encryption could have avoided a majority of breaches. |
| 14 | G:\Meaningful Use\HITPC\Stage\_3\_RFC\Submission | p.1 |  | VA | * Invalid link. Cannot view document. |
| 15 | [HHS-OS-2012-0007-DRAFT-0051](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0051) | p.1 | Peter Alterman | SAFE-BioPharma Association | * No response. |
| 16 | [HHS-OS-2012-0007-0210](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0210) | p.11 | Linda  Brady | ADHI | * Commented that absolutely EPs/EHs/CAHs should attest to implementing all portions of the HIPAA Security Rule. * Recommended including a requirement for encryption, because encryption is not being done on a consistent basis until a breach has occurred. * Suggested that encryption be required for certification and be sure it cannot be bypassed or turned off in the system. |
| 17 | [HHS-OS-2012-0007-0203](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0203) | p.11 | Robert  Bennett | American Academy of Family Physicians | * Observed if Health Insurance Portability and Accountability Act (HIPAA) compliance is a problem, then obviously HIPAA is not having the intended impact. * Suggested using HIPAA, not meaningful use, to improve privacy and security education, policy, and process. |
| 18 | [HHS-OS-2012-0007-0503](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0503) | p.11 |  | The Joint Commission | * Commented that it believed that it is appropriate for providers and hospitals to attest that they are conforming to the Healthcare Insurance Portability and Accountability Acts (HIPAA) Security Rule. * Commented that it believed that attestation would not cause burden on the entities as they should already be in conformance. Further, if they are not it will provide another opportunity for the government to stress the importance of the rule. * Commenter remarked that it required its ORYX vendors to attest that they (1) adhere to HIPAA and all related regulations and guidance; (2) have policies and procedures that address security protocols; (3) have policies, procedures, and practices that address employee and other authorized individuals access, use, disclosure, and safeguarding of Protected Health Information; and (4) provide initial and annual training to their employees and any authorized individuals related to the organization’s administrative, physical, and technical policies, procedures, and practices for all technical reporting requirements related to the ORYX contract agreement. |
| 19 | [HHS-OS-2012-0007-0325](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0325) | P.12 | Pamela  Foyster | Quality Health Network | * Stated that the Security Rule is a good idea. * Was undecided on attestation (commenter was in favor of attesting “attest Yes/No”). |
| 20 | [HHS-OS-2012-0007-0279](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0279) | p.17 | Yomaris  Guerrero | Boston Medical Center | * Supported requiring attestation to the implementation of HIPAA Security Rule provisions regarding workforce/staff outreach and training. * Recommended access control and identity management as very important aspects. * Believed entities should be able to demonstrate proper role based access control design as hospital systems in general are very open in nature. |
| 21 | [HHS-OS-2012-0007-0506](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0506) | p.19 | Jamie Ferguson | Kaiser Permanente | * Stated that the current HIPAA Security Rule requirement to conduct or review a security risk assessment is comprehensive and clearly requires providers to comply with all of its provisions. * Commented that it would be unnecessary and overly burdensome to require attestation under the MU Program for specific components of the Rule such as security training and workforce awareness. |
| 22 | [HHS-OS-2012-0007-0342](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0342) | p.4 | Adolph  Maren Jr. | Oklahoma Health Care Authority | * Supported the proposal for attestation of training workforce on the practical implications of the HIPAA Security Rule. * Commented that a number of security issues through provider use of unencrypted mobile devices, such as iPads and smart phones, and non-HIPAA compliant applications such as Facetime and Skype. * Recommended that training of regulations as they apply to mobile devices and communications be required as part of the proposed workforce / staff outreach and training attestation. |
| 23 | [HHS-OS-2012-0007-0510](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0510) | p.2 | Kelly Broder | Surescripts, LLC | * Stated that the HIPAA Security Rule provides the appropriate baseline information security standards for the development of EHRs, and additional requirements that go beyond these HIPAA provisions are unwarranted. * Stated that ONC should not include additional security steps as a component of a meaningful use attestation, because both the authority of the OCR in this area and the need for all meaningful use participants to meet these core HIPAA standards. * Commented that covered entities are required by the HIPAA Security Rule to conduct ongoing risk assessments and engage in specific risk management steps, and these required steps cover EHRs in the same way that the HIPAA Security Rule governs all other aspects of the health care system for covered entities and their business associates. * Commented that there is no need for additional, supplemental or highlighted requirements as part of any particular aspect of the operation of a health care entity’s business. |
| 24 | [HHS-OS-2012-0007-0486](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0486) | p.2 | Tina Grande | The Confidentiality Coalition | * Did not object to guidance or advice issued by the HHS Office of Civil Rights related to the HIPAA Security Rule. * Did not object to ONC issues its own guidance about recommendations for steps related to security risk analysis or other aspects of the HIPAA Security Rule, in the appropriate context. * Did not believe that ONC should include additional security steps as a component of a meaningful use attestation, because the HIPAA Security Rule will apply to any entity seeking meaningful use incentives (as a HIPAA covered entity). * Commented that the requirements for risk assessment, risk management and risk mitigation are required by the HIPAA Security Rule are obligations of every covered entity (and shortly will be, as well, for all business associates). * Commented that training is an important aspect of any kind of compliance, but asserts that there is no value in singling out any particular element of the HIPAA Security Rule as deserving more attention than others or imposing additional obligations related to any particular requirements, even if compliance problems have been identified in the past. * Stated that the HIPAA standard, with its risk-focused approach, is sufficient to address the full range of information security concerns raised by electronic health records. * Commented that there is no need for additional, supplemental or highlighted requirements as part of any particular aspect of the operation of a health care entity’s business. * Stated that Congress has spoken on its desired changes to the HIPAA structure, and asserts there is no basis at this time to go beyond Congressional intent (which has not yet even been implemented in full) to impose a broader set of changes. * Suggested if ONC does in fact propose new privacy and security standards that affect electronic health records or health information exchange (HIE) activity more broadly, then it should delay any such efforts until HITECH has been finalized and implemented. |
| 25 | [HHS-OS-2012-0007-0565](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0565) | p.21 | Leigh  Burchell | Allscripts | * Agreed that employee training and other administrative controls from the HIPAA Security Rule are important. * Commented that employee training and other administrative controls should not have an impact on EHR certification. |
| 26 | [HHS-OS-2012-0007-0493](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0493) | p.27 | Thomas Merrill | New York City Department of Health and Mental Hygiene | * Stated that demonstrating that staff is appropriately trained should be a requirement. * Commented that in an audit, the provider would have the burden of demonstrating that each employee is appropriately trained. * Commented that a verification of training in the employee personnel file might be more effective than requiring an additional attestation. |
| 27 | [HHS-OS-2012-0007-0505](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0505) | p.27 |  | Pharmacy e-HIT Collaborative | * Supported current HIPAA security rule provisions. |
| 28 | [HHS-OS-2012-0007-0274](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0274) | p.28 | Thomson  Kuhn | American College of Physicians | * Stated that the key to any such activity is the availability of truly useful education materials on the security rule to guide practices to the desired performance. * Commented that small practices lack the expertise needed to design and deliver such programs and therefore, must typically rely on outside sources of such content. * Did not want practices having to pay for consultants to come in and deliver programs, which would add considerable expense to maintaining compliance. |
| 29 | [HHS-OS-2012-0007-0321](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0321) | p.28 | Linda  Fishman | American Hospital Association | * Believed that the meaningful use rule should not be used as a means to enforce compliance with all HIPAA privacy and security requirements, including those for making staff and workforce members aware of the HIPAA Security Rule and to train them on Security Rule provisions. * Believed that meaningful use attestation about implementing the HIPAA rules is unnecessary. * Commented that it is the Office of Civil Rights (OCR) that regulates and enforces HIPAA, and using the meaningful use rules as a back-up mechanism for enforcement is inappropriate and may lead to a potentially different or conflicting set of compliance obligations enforced by multiple agencies through multiple and uncoordinated means. * Suggested the HITPC to reject requirements for EPs/EHs/CAHs to attest to implementing HIPAA Security Rule provisions regarding workforce/staff outreach and training and sending periodic security reminders. |
| 30 | [HHS-OS-2012-0007-0350](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0350) | p.3 | Landon  Combs | Highlands Physicians Inc | * Agree to attestation * Suggested providing online access to classes/Data to help people train/track. * Suggested this could also incorporate into welcoming message. |
| 31 | [HHS-OS-2012-0007-0533](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0533) | p.31-32 | Lindsey  Hoggle | Academy of Nutrition and Dietetics | * Was concerned that there is still significant confusion in the medical profession as to the provisions of HIPAA. * Stated that if patients are to understand security risks of accessing their own data online, it seems that a consistent culture of security awareness amongst providers (in all areas of care) is necessary. * Suggested attestation under MU will support the continued need for Security Training among all health care staff. * Stated that proof of security reminders should be a requirement. |
| 32 | [HHS-OS-2012-0007-0315](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0315) | p.33 | Angela  Jeansonne | American Osteopathic Association | * No response. |
| 33 | [HHS-OS-2012-0007-0568](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0568) | p.33 | Sasha  TerMaat | Epic | Providers and hospitals will provide the best feedback on this  question. |
| 34 | [HHS-OS-2012-0007-0306](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0306) | p.33 | Julie  Cantor-Weinberg | College of American Pathologists | * Did not believe that ONC should include additional security steps as a component of a meaningful use attestation. * Utilized the idea of training as a potential element of an attestation, based on HIPAA compliance reviews that identified certain weaknesses in compliance related to training. * Acknowledged training is an important aspect of any kind of compliance, but sees no value in singling out any particular element of the HIPAA Security Rule as deserving more attention than others or imposing additional obligations related to any particular requirements. * Suggested that if ONC does in fact propose new privacy and security standards that affect electronic health records or health information exchange (HIE) activity more broadly, then it should delay any such efforts until HITECH has been finalized and implemented. |
| 35 | [HHS-OS-2012-0007-0212](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0212) | p.34 | Kari  Guida | Minnesota Department of Health | * Commented that mobile health and user-provided device should be considered. |
| 36 | [HHS-OS-2012-0007-0502](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0502) | p.36 | Clara Evans | Dignity Health | * Believed that the meaningful use rule should not be used as a means to enforce compliance with all HIPAA privacy and security requirements, including those for making staff and workforce members aware of the HIPAA Security Rule and to train them on Security Rule provisions. * Believed that meaningful use attestation about implementation of HIPAA rules is unnecessary and recommend HITPC allow the Office of Civil Rights (OCR) to continue regulating and enforcing HIPAA. * Urged the HITPC to reject requirements for EPs/EHs/CAHs to attest to implementing HIPAA Security Rule provisions regarding workforce/staff outreach and training and sending periodic security reminders. |
| 37 | [HHS-OS-2012-0007-0569](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0569) | p.37 | Del  Conyers | Heart Rhythm Society | * No Comment |
| 38 | [HHS-OS-2012-0007-0588](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0588) | p.46 | Gregory  Rivas | UC Davis Medical Center | * Did not have issues. Noted that UCDMC is currently mandating this training. |
| 39 | [HHS-OS-2012-0007-0332](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0332) | P.5 | Patrick  Sullivan | Harris Corporation | * Noted that there is 5 years of data on covered entity noncompliance. * Recommended that HITPC require EPs/EHs/CAHs to attest to implementing HIPAA Security Rule provisions, at least to address the top 5 areas of noncompliance. |
| 40 | [HHS-OS-2012-0007-0536](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0536) | p.5 | David  Harlow | Society for Participatory Medicine | * Suggested action on provider education. * Suggested that provider staff should be trained on the rights of patients to access their own health care information as part of their HIPAA training. |
| 41 | [HHS-OS-2012-0007-0346](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0346) | p.5 | American Academy of Dermatology Association |  | * Had concerns that many practices and other provider organizations are being challenged to meet standards on privacy and security of patient information as prescribed by both meaningful use and the Health Insurance Portability and Accountability Act (HIPAA). * Believed that transmission and exchange of patient data or information across the enterprise must be very solid and secure. * Recommended against requiring that physicians attest to implementing HIPAA Security Rule provisions regarding workforce/staff outreach & training and sending periodic security reminders. * Suggested that awareness of staff of the HIPAA Security Rule provisions superficially speaks to HIPAA compliance, but it does not address the substantive technological issues of keeping information secure. For example, use of mobile devices to generate and communicate health information subjects this potentially sensitive information to increased security risks, and the security risks presented by these transmissions must be adequately addressed. Successfully engaging in meaningful use will require expanded focus on secure transmission of data within and outside of the enterprise. * Urged the HITPC to give greater attention to existing technological deficiencies that foster security breaches. * Recommended that CMS or the Office of the National Coordinator provide additional educational resources on HIPAA to small physician practices. |
| 42 | [HHS-OS-2012-0007-0333](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0333) | P.50 | Koryn  Rubin | American Association of Neurological Surgeons and Congress of Neurological Surgeons | * Recommended preservation of the requirement that meaningful users meet HIPAA Security Rule requirements. * Suggested developing tools, such as webinars, PowerPoint presentations and YouTube videos to assist with understanding the HIPAA Security Rules. |
| 43 | [HHS-OS-2012-0007-0541](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0541) | p.51 | John  Glaser | Siemens Healthcare | * Recommended focusing on administration, policy, and procedures, as these are highlighted in the HIPAA Security Rule. * Suggested that the management of these processes should not be considered part of EHRT, but rather part of education or security management systems that can track who was trained, notifications, refresher courses, etc. and becomes more of an attestation or proof of compliance from EH/EP/CAH. |
| 44 | [HHS-OS-2012-0007-0145](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0145) | p.53 | Nancy  Payne | Allina Health | * Commented that human behavior is a very important part of good security. * Stated that education is a good part of the rule to focus on. * Suggested that education remains as an attestation only measure. |
| 45 | [HHS-OS-2012-0007-0561](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0561) | p.57 | Emily  Graham | Alliance of Specialty Medicine | * Recommended preservation requirements for meaningful users to meet HIPAA Security Rule requirements. * Suggested developing tools, such as webinars, PowerPoint presentations and YouTube videos to assist with understanding the HIPAA Security Rules. |
| 46 | [HHS-OS-2012-0007-0295](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0295) | p.7 | Susan  Owens | Memorial Healthcare System | * Stated that Security Awareness Training should be mandatory because it is essential. * Stated the importance of requiring regular and consistent Access Review for all users. * Stated the importance of requiring encryption at rest and in transit. |
| 47 | [HHS-OS-2012-0007-0327](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0327) | P.7 | Megan  Howell | Group Health Cooperative | * Suggested requiring a Security Awareness Program that encompasses the HIPAA Security Rule requirements as part of an organization’s overall Information Security Program (by default). * Observed that attestation should not add significant overhead to the overall attestation effort. |
| 48 | [HHS-OS-2012-0007-0520](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0520) | PDF2 - p.78 | Andy Riedel | NextGen Healthcare | * Noted that commenter agreed that employee training and other administrative controls from the HIPAA Security Rule are important. * Did not believe that training and other administrative controls need to be added to meaningful use attestation. * Commented that training and such are already HIPAA obligations. * Stated that, as a matter of principle, meaningful use should not attempt to duplicate existing regulatory requirements. |
| 49 | [HHS-OS-2012-0007-0547](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0547) | tab 3 | Erin  Laney | Intermountain Healthcare | * Did not object if ONC wishes to require attestation of compliance with the areas of workforce/staff outreach. * Suggested that ONC should not provide guidance or introduce interpretation of the Security Rule independently. * Suggested that ONC should rely solely on the guidance and interpretation of the rule as published by the OCR when crafting certification criteria for MU3. * Commented that it is in the interest of neither the healthcare industry nor ONC to have two federal agencies enforcing conflicting requirements, therefore ONC should strive to reject divergence from or enhancement to the OCR published interpretive guidance of the Security Rule. * Stated that ONC not require attestation for addressable requirements in such a way that it interferes with the flexible intent of the Security Rule. * Suggested that ONC should not restrict the right of MU3 participants to select solutions that are reasonable and feasible for their specific environments. * Emphasized along with many in the industry that the Security Rule will apply to EMR systems regardless of ONC's reiteration of those requirements in the detail of the certification criteria. * Suggested OCR to use caution as it considers inclusion of Security Rule requirements if conflicts with the OCR interpretation may result. * <http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0547> |
| 50 | [HHS-OS-2012-0007-0535](http://www.regulations.gov/#!documentDetail;D=HHS-OS-2012-0007-0535) | tab 4 | Dan  Rode | American Health Information Management Association | * Suggested that ONC continue to rely on OCR process to review and define the specific criteria. * Stated that having more specific criteria in meaningful only bring inconsistencies between MU and the Privacy and Security rules. * Stated that if more specific criteria is required, this should be given back to the OCR to update the Privacy and Security Rule. * Recommended that EPs/EHs/CAHs attest to meeting the HIPAA Privacy and Security rules, and let OCR be more prescriptive and change the Privacy and Security rules as needed. |

**Summary**

**Number of Comments:** 46 (4 commenters did not include a response or link was invalid)\_

**Summary:**

**Key Issues:** Commenters identified the following safeguards to be emphasized in MU 3 and key areas highlighted around training for the workforce.

* Access controls (1)
* Audits (1)
* Data integrity (2)
* Encryption:
  + Encryption (2)
  + Encryption of data on removable media (1)
  + Encryption at rest (1)
  + Encryption in transit (1)
  + Full-disc encryption of mobile devices accessing EHRs (2)
  + Transmission of patient information, both inside and outside enterprise (1)
* Identity management (1)
* Implementation of backup and recovery plans (1)
* Policies and procedures related to prevention of local storage of PHI (1)
* Malware on all workstations accessing EHRs and EHR modules (1)
* Social media, bring your own device (BYOD), and mobile devices (1)
* Specific security controls in place (if local data storage) (1)
* Training on specific areas:
  + Assignment and training on Security Officer role (1)
  + Mobile device security (2)
  + More timely and targeted training on security (1)
  + Patient’s Right of Access (1)
  + Security controls (1)
  + Usability of security solutions (1)
  + Workforce security training (general) (4)
* More guidance and education for providers on HIPAA Security Rule (e.g., to understand encryption, risk assessment, risk mitigation) (4)

**Requiring Attestation:** Commenters included those for, against and neutral regarding the addition of an attestation for workforce security training. Those against adding such an attestation, most frequently cite that such an attestation is either burdensome or duplicative of the HIPAA Security Rule. Those commenters who support adding an attestation requirement for EHs/EPs/CAHs for workforce training most frequently cite the importance of the workforce in keeping patient health information secure.

* Requirement for Attestation is focused on:
  + Commonly neglected HIPAA Security Rule provisions (1)
  + Workforce training provided (11)
    - Training attestation is burdensome and/or duplicative to HIPAA requirements (15)
  + Implementation of all portions of HIPAA Security Rule (2)
* Defer to providers on MU Attestation for training (1)
* Support current HIPAA Rule Security provisions (no reference and/or objection to attestation) (6)

**Other:**

* Clearly delineate security requirements/certification criteria for software platform versus actual users of EHR.

**Appendix:**

* Access controls (#20)
* Audits (#12)
* Data integrity (#3, #7)
* Encryption:
  + Encryption (#13, #16)
  + Encryption of data on removable media (#5)
  + Encryption at rest (#47)
  + Encryption in transit (#46)
  + Full-disc encryption of mobile devices accessing EHRs (#2, #5)
  + Transmission of patient information, both inside and outside enterprise (#41
* Identity management (#20)
* Implementation of backup and recovery plans (#2)
* Policies and procedures related to prevention of local storage of PHI (#4)
* Malware on all workstations accessing EHRs and EHR modules (#2)
* Social media, bring your own device (BYOD), and mobile devices (#3)
* Specific security controls in place (if local data storage) (#4)
* Training on specific areas:
  + Assignment and training on Security Officer role (#7)
  + Mobile device security (#22, #35)
  + More timely and targeted training on security (#3)
  + Patient’s Right of Access (#40)
  + Security controls (#3)
  + Usability of security solutions (#3)
  + Workforce security training (general) (#2, #9, #25, #38)
* More guidance and education for providers on HIPAA Security Rule (e.g., to understand encryption, risk assessment, risk mitigation) (#8, #41, #42, #45)