GOVERNMENT HEALTH IT

March 29, 2013

Commentary: The litigation and risk-management concerns meaningful use triggers

James M. Hofert, Partner, Hinshaw & Culbertson LLP and **Roy M. Bossen,** Partner, Hinshaw & Culbertson LLP and **Linnea L Schramm,** Associate, Hinshaw & Culbertson LLP and **Michael A. Dowell,** Partner, Hinshaw & Culbertson LLP

New federal healthcare legislation and implementing regulations seek to exert control over aspects of patient care, from outlining the substantive information that healthcare providers should obtain from their patients to specification of treatment algorithms a physician should consider once a diagnosis is made.

Meaningful use standards require healthcare providers to affirmatively act to identify potential future health risks in patients seen for unrelated health conditions. New regulations also require continued patient follow-up after discharge from care to ensure compliance with care directives. The regulations reflect laudable goals but create significant potential risk for malpractice claims for unwary healthcare providers.

Thus far, great concern has been expressed as it relates to physician and institutional liability if information systems are hacked or if cloud-based products are illegally accessed. CHIME noted that there are significant program issues relating to system interfaces so as to allow communication of EHR between physicians and other institutions. Multiple industry associations have suggested that implementation of Stage 3 be delayed by up to two years to allow for evaluation of the impact of Stages 1 and 2 on the healthcare system.

The emphasis that has been placed on the adoption of information technology in the healthcare field in the last several years, meanwhile, generates potential legal and risk management concerns. As the requirements for acceptable EHR systems evolve, so do relevant common law standards of care. The rapidity with which healthcare institutions must develop and implement EHR systems to meet "meaningful use" criteria presents significant risk for malpractice claims.

Initial transition from paper to electronic record systems can create risk of: implementation errors (software issues); inadequate training issues; incorrect or inconsistent use; and individual mistakes in the creation of the electronic record. The use of both paper and electronic records may create documentation gaps leading to misdiagnosis and inappropriate treatment. Procedures must be developed for confronting problems in the implementation of electronic recordkeeping. Consistent standardized use of developing electronic systems is imperative.

Meaningful use requirements relating to the need to document and treat a patient's future health risks creates a gray area as to what, if any, responsibility institutions and physicians have in evaluating patients for potential health issues unrelated to the reason for hospital admission and/or treatment. Regulatory requirements relating to coordination of post-hospital care creates obligations to provide services in a reasonable manner, including follow-up where provider/patient communication potentially becomes a significant problem.

The use of electronic communication systems to diagnose and treat patients remotely creates a potential malpractice risk. There is a clear risk of misdiagnosis associated with remote treatment. There is also litigation risk in relation to the failure to properly follow-up.

Healthcare providers will need to create and implement guidelines with respect to use of electronic communication systems in treating patients' health complaints or concerns.

Hospital substantive treatment guidelines, i.e., clinical decision support guidelines, must be carefully drafted as they create the potential for institutional liability and can potentially negate agency defenses presently enjoyed by many healthcare institutions. Additionally, failure to oversee use of clinical guidelines once in place creates potential institutional liability. Moreover, a physician's override of an alert by implementing a nonconforming treatment plan creates potential liability for both the physician and institution.

Beyond this, the ability to access historic inpatient and outpatient records creates a potential duty to review same regardless of the reason that a physician may be seeing the patient. A failure to adopt an integrated EHR system may, itself, constitute a breach of the standard of care. Evolution of EHR systems creates a continued duty to communicate and train users.

Patient stewardship is a laudable goal but presents significant litigation risk. Lack of definition of which care provider has the duty to comply with given meaningful use criteria further confounds liability issues. Controls must be implemented to manage financial and liability risks associated with common law malpractice actions arising out of HITECH compliance.

GOVERNMENT HEALTH IT

May 1, 2013

Commentary: Delving into HIPAA breach notification

James M. Hofert, Partner, Hinshaw & Culbertson LLP and **Roy M. Bossen,** Partner, Hinshaw & Culbertson LLP and **Linnea L Schramm,** Associate, Hinshaw & Culbertson LLP and **Michael A. Dowell,** Partner, Hinshaw & Culbertson LLP

The U.S. Department of Health and Human Services (HHS) recently issued its Final Rule designed to strengthen the privacy and security protections for individual health information. The Final Rule, among other things, modified the breach notification requirements and enforcement provisions to "improve the workability and effectiveness, and to increase flexibility for, and decrease burden on the regulated entities." While the Final Rule's effective date was March 26, 2013, Covered Entities and Business Associates have until September 23, 2013, to come into compliance with it.

This article will discuss the Final Rule's breach notification requirements and HIPAA privacy and security enforcement provisions. Readers should note that these are but two of the important areas covered under the Final Rule, and that significant changes have been made to the notice of privacy practices under HIPAA, that there are new requirements for Business Associates and their subcontractors, and that other important modifications have been made to the Privacy Rule affecting marketing, fundraising, sale of protected health information (PHI), and other matters.

The Health Information Technology for Economic and Clinical Health Act (HITECH) amended the Health Insurance Portability and Accountability Act (HIPAA) to require that Covered Entities provide notification to affected individuals and to the U.S. Secretary of HHS following discovery of a breach of unsecured PHI. In some instances, a Covered Entity would be required to notify media in the case of breaches of unsecured PHI of more than 500 instances. HITECH also required that the Business Associates of Covered Entities notify the applicable Covered Entity of the breach.

Under the old HIPAA breach rules, there were three situations in which exceptions to the notification requirements applied:

(1) the PHI was unintentionally accepted by a workforce member performing his or her duties; (2) the PHI was inadvertently disclosed from one workforce member to another; and (3) the PHI was disclosed to a person who reasonably would not have been able to obtain that information. Under the third exception, Covered Entities were to perform a risk assessment to determine whether the impermissible use or disclosure posed a significant risk of financial, reputational or other harm to the individual. Thus, if a Covered Entity could show that it took immediate steps to mitigate an impermissible use or disclosure, such steps could be used to argue that the Covered Entity reduced the risk to less than a significant risk of financial, reputational or other harm.

Such remedial steps would include activities to ensure that information would not be further used or disclosed, including possibly having the inadvertent recipient of the PHI returning or destroying it. If such steps eliminated or reduced the risk of harm to an individual to less than a "significant risk," then under the previous rule it could be interpreted that the security and privacy of the information was not compromised and, therefore, that no breach notification was required.

The Final Rule maintains two of the three statutory exceptions, and modifies the third. Under the Final Rule, a breach excludes any unintentional acquisition, access or use of PHI by a workforce member, or a person acting under the authority of a Covered Entity or Business Associate if such acquisition, access or use was made in good faith and was in the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule. The second exception indicates that a breach does not include inadvertent disclosures of PHI from a person who is authorized to access PHI of a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate.

As a result of significant comments obtained by HHS in the comment period, and after considering those public comments, HHS amended the third exception in its Final Rule. By modifying the risk assessment approach, HHS added language to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity or Business Associate shows a low probability that the PHI has been compromised. This "low probability" standard replaces the "significant risk of financial, reputational or other harm" standard. Thus, under the new standard, a breach notification would be required in all situations, except where the Covered Entity or Business Associate could show that there was a low probability that the PHI had been compromised, or that the workforce exceptions discussed above apply. In order to show that there is a low probability of disclosure, the Final Rule identifies other factors that Covered Entities and Business Associates should consider when performing a risk assessment to determine if the PHI has been compromised and breach notification is required.

The Final Rule requires that the following four factors be considered when conducting the risk assessment. Covered Entities and Business Associates should modify their policies and procedures to ensure that when they evaluate the risk of an impermissible use or disclosure, all four are considered.

1. The first factor to be considered when conducting the risk assessment concerns the nature and extent of the PHI involved, including the type of identifiers and likelihood of re-identification. When conducting a risk assessment, the nature and degree of any clinical information used or disclosed must be considered. Examples given

in the Commentary to the Final Rule indicate that when assessing clinical information disclosed, the entity must consider not only the nature of the services or other information, but also the amount of detailed clinical information involved — for example, treatment plans, diagnosis, medication, medical history, etc. The consideration of the type of PHI involved in a possible breach should help Covered Entities or Business Associates determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual. Additional factors that could be considered include whether there are direct identifiers in the impermissible used or disclosed information, and whether there was a likelihood that the PHI released could be re-identified based on context or ability to link up to other information.

2. The second factor to be considered when conducting the risk assessment requires Covered Entities and Business Associates to determine the identity of the unauthorized person who impermissibly used the PHI, and to whom the impermissible disclosure was made. Thus, for example, if an impermissible disclosure of PHI was made to another Covered Entity obligated to comply with HIPAA, there may be a low probability that the PHI would be compromised since the recipient is also obligated to protect PHI. The Commentary to the Final Rule suggests that if the information that is impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the PHI has the ability to re-identify the information.
3. The third factor to be considered when conducting the risk assessment requires Covered Entities and Business Associates to investigate an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, whether the opportunity existed for the information to be acquired or viewed. Consequently, if a laptop computer is stolen and later recovered, and a forensic analysis indicates that the PHI was never accessed, viewed, acquired, transferred or otherwise compromised, the Covered Entity would be able to determine if the information was not actually acquired by an unauthorized individual. Contrast that situation, however, with one where a Covered Entity mails information to the wrong individual, who opens it and calls the entity to say that he or she received the information. In such case, the unauthorized recipient viewed and acquired the information because he or she opened and read it.
4. The fourth factor to be considered when conducting the risk assessment requires Covered Entities and Business Associates to consider the extent to which the risk has been mitigated. Covered Entities and Business Associates must attempt to mitigate risk following impermissible uses or disclosure. Such mitigation could include assurances that the information would not be further used or disclosed, through a confidentiality agreement or similar means, as previously suggested in the original rule, or that the information will be destroyed. Covered Entities and Business Associates should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

In the Commentary to the Final Rule, it is suggested that this last factor should be considered in combination with the other factors regarding the unauthorized recipient of the PHI disclosed. The Commentary indicates that a Covered Entity or Business Associate's analysis of the probability of PHI being compromised must address each of the four factors. If, after evaluating in accordance with the above, the Covered Entity or Business Associate cannot determine that there was a low probability that the PHI has been compromised, then a breach notification is required.

The Final Rule maintains the provisions regarding when a breach is deemed discovered, and the timing and content of the required notification. It modifies the point by which Covered Entities are required to notify the Secretary of HHS of all breaches of unsecured PHI affecting fewer than 500 individuals to not later than 60 days after the end of the calendar year in which the breaches were discovered, rather than 60 days from the end of the calendar year. It should be noted that Covered Entities and Business Associates have the burden of proof to demonstrate that all notifications were provided, or that impermissible use or disclosures did not constitute a breach. Covered Entities must maintain documentation of their analysis. Thus, a risk assessment demonstrating that there was a low probability that PHI was compromised or that it was impermissibly used or disclosed should be documented and maintained and should show that the information fell within one of the exceptions.

The Final Rule also strengthened the enforcement provisions by increasing penalties for HIPAA and HITECH violations. HHS has established four categories of violations that reflect increased culpability. These levels of violation include: (1) did not know; (2) reasonable cause; (3) willful neglect corrected; and (4) willful neglect not corrected. For each of these categories there is a penalty for violation and a provision for a maximum for all violations of an identical provision in a calendar year.

Penalties apply to both Covered Entities and Business Associates, including subcontractors, and will be determined on a case-by-case basis, with the HHS Office for Civil Rights considering the nature and extent of the violation, the nature and extent of the resulting harm, and the entity's history of non-compliance when determining penalties. HHS has also indicated that the entity's financial position will be examined and that the agency will consider prior non-compliance, even if there has been no formal finding of a violation.

The Final Rule also provides that: (1) the Secretary of HHS is required to investigate any complaint if a preliminary review of facts indicates a possible violation due to willful neglect; (2) the Secretary is required to conduct a compliance review when a preliminary review indicates a possible violation due to willful neglect; and (3) the Secretary may attempt to resolve investigations or compliance review indicating non-compliance by informal means.

Finally, Covered Entities and Business Associates are liable for their Business Associate agents' acts, even if the Covered Entity has a Business Associate agreement in place. Key questions to assess are: (1) whether the Business Associate engaged in a course of conduct subject to control by the Covered Entity; (2) whether the Business Associate's conduct is commonly performed to accomplish the services performed on behalf of the Covered Entity; and (3) whether the Business Associate activity was reasonably expected by the Covered Entity. Thus, it is important to take steps to avoid agency relationships wherever possible, and to include clear indemnification provisions when Covered Entities contract with Business Associates. These increased enforcement activities and provisions require Covered Entities and Business Associates to review their policies and procedures to ensure that they incorporate necessary safeguards.

GOVERNMENT HEALTH IT

June 25, 2013

Commentary: Concerns about quality improvement organizations actions around meaningful use

James M. Hofert, Partner, Hinshaw & Culbertson LLP and **Roy M. Bossen,** Partner, Hinshaw & Culbertson LLP and **Linnea L Schramm,** Associate, Hinshaw & Culbertson LLP and **Michael A. Dowell,** Partner, Hinshaw & Culbertson LLP

The federal government is pressuring the medical community to reduce patient care costs while improving the quality of patient care to all patients, including Medicare beneficiaries. Congress, recognizing that hospital readmissions are too common and are costly and often avoidable, passed the Hospital Readmission Reduction Program (HRRP), which ties-in readmission metrics to monetary penalties to encourage hospitals to reduce readmission rates. Federal lawmakers also passed the Health Information Technology for Economic and Clinical Health Act (HITECH), which is intended to stimulate the rapid evolution and adoption of information technology in the healthcare industry, promote the development and use of clinical decision support (CDS) treatment algorithms, encourage active provider participation in discharge planning and care to decrease recidivism, and enhance care coordination through provider-patient communication.

Consistent with these legislative strategies, the Center for Medicare and Medicaid Services (CMS) appears to be encouraging contracted quality improvement organizations (QIOs) to adopt quality care principles (meaningful use criteria), created pursuant to HITECH, as additional criteria to be applied in the evaluation of the adequacy of care provided to Medicare beneficiaries under their jurisdiction.

In 1982, Congress established utilization and quality control peer review organizations (PROs) (now known as QIOs) to perform two broad functions: (1) promote quality health care services for Medicare beneficiaries; and (2) determine whether services rendered are medically necessary, appropriate and meet professionally recognized standards of care. The goal of the QIO program is to improve medical outcomes for Medicaid beneficiaries.

QIOs have recently targeted psychiatrists as well as safety-net hospitals, along with other covered institutions providing inpatient psychiatric care; reviewing both the adequacy of the care provided as well as the appropriateness of the discharge planning pursuant to Section 1156 of the Social Security Act. QIOs are applying "meaningful use" criteria adopted pursuant to HITECH to assess whether the physicians and institutions being reviewed are acting in accord with professionally recognized standards of care. QIOs such as Telligen, LLC (formerly IFMC Illinois) have issued sanction notices suggesting substantial violations of Section 1156 for a providers' failure to meet "meaningful use" criteria. QIOs appear to be applying a higher level of scrutiny to cases where patients are readmitted to the same or another institution within 30 days.

QIOs such as Telligen have essentially associated the principle of "professionally recognized standards of care" under Section 1156 with "meaningful use criteria" enunciated under HITECH along with other historically applied principles of care. The term "professionally recognized standard of care" is not specifically defined by regulators (the Quality Improvement Organization Manual suggests that the term may be equated to evidence-based practices and/or documented consensus statements, best practices and/or identified norms).

The failure of a physician, hospital or other covered institution to implement acceptable corrective action plans can lead to financial penalties or exclusion from reimbursement for services rendered to Medicare patients. This remedy goes beyond HITECH provisions, which simply provide that institutions not presently in compliance are not entitled to incentive payments.

Recent actions by QIOs like Telligen, requiring covered facilities — including safety-net institutions — to meet "meaningful use" criteria under HITECH creates significant concerns. While the intent of HITECH is to promote implementation of electronic record systems and the adoption of clinical decision support (CDS) algorithms and enhanced care coordination through provider communication, implementation of HITECH "meaningful use" criteria is to be staged through 2016. Regulators have recognized that physicians and other covered providers need time to implement electronic record systems and required protocols.

Major medical associations such as the American Medical Association (AMA), American Academy of Family Physicians (AAFP), College of Healthcare Information Management Executives (CHIME), and the HIMSS Electronic Health Record Association (EHRA), have all expressed concern

about the implementation of Stage III meaningful use criteria by 2016. They cite ongoing problems in implementing EHR systems and in integrating the use of these systems throughout various healthcare networks and suggest that CMS has failed to adequately assess the impact of Stage I meaningful use criteria on hospital operations. The associations also note that there has been no evaluation of Stage II meaningful use criteria, in that these criteria have not yet been implemented. It is these criteria that impose patient stewardship responsibilities and require extensive discharge planning and follow-up. The associations suggest postponing implementation of Stage II and Stage III meaningful use criteria.

Contractors have recently devoted substantial attention to psychiatric admissions to safety-net hospitals. During the review process, Telligen alleged concerns ranging from the failure to: (a) stabilize patients prior to discharge/transfer; (b) arrange for adequate follow-up care; (c) address issues of readmission and recidivism; (d) the taking of appropriate legal action to compel administration of psychotropic drugs or involuntary admission. Each of the alleged concerns/violations were based in part on HITECH "meaningful use" criteria relating to EHR systems, clinical decision support (CDS) protocols as enunciated by the Telligen reviewer or "use" criteria relating to discharge policies and procedures including follow-up.

Respondent physicians and institutions implicated during this process have pointed to regulatory limitations on the ability to subject patients to involuntary admission or administration of psychotropic medication, and regulations restricting admission to acute care hospitals where alternative facilities would otherwise provide sufficient care. Respondents have also cited American Psychiatric Association (APA) guidelines relating to the need to treat patients through alternative community programs where possible. They also argued that many of the subject patients had significant social risk factors compounding discharge planning and follow-up care.

Many of the institutions cited will face significant challenges because they operate under slim financial margins compared to other institutions. In several recent cases pursued by Telligen, institutions felt compelled to adopt corrective action plans for which they lacked adequate staff and resources because of the draconian nature of the sanctions that could be imposed.

Independent research conducted by the Commonwealth Fund supports the respondents' concerns. Commonwealth Fund studies suggest that safety-net hospitals are 30 percent more likely to have 30-day readmission rates above the national average. Hospitals serving large numbers of low-income patients are more likely to have the lowest adjustment factors and receive the maximum penalty of 1 percent under HRRP. The same institutions are at risk to not receive Medicare and Medicaid incentive payments under HITECH and face potential imposition of penalties under that legislation if their failure to comply continues through 2015. Further imposition of sanctions by QIOs for failure to meet "meaningful use" criteria, not yet implemented and evaluated by CMS, compounds an already complicated regulatory picture for hospitals in general, and for safety-net institutions in particular.

Safety-net institutions handle a disproportionate share of vulnerable populations that include low-income insureds, underinsureds or patients on Medicaid. Safety-net hospital patients have substantially higher rates of chronic health problems, disability, mental illness and substance abuse compared to the general population. They also have disproportionate personal and social needs adversely affecting their health and otherwise imposing roadblocks to coordinated care. These include homelessness, unsafe housing, unstable employment and lack of family support. This population requires significant enabling and support services and transitional care post-discharge, which may well be beyond safety-net institutions' ability to provide.

QIOs should be circumspect in sanctioning physicians and covered institutions for violation of "meaningful use" criteria that has yet to be implemented or fully evaluated by CMS. QIOs may need to consider application of a "sliding scale" assessment, at least initially, as it relates to application of "meaningful use" criteria during care reviews, to allow nonuniversity based hospitals as well as safety-net institutions, the necessary time to bring themselves into compliance with evolving EHR, CDS and discharge planning and care requirements incorporated into recently passed healthcare legislation.

HINSHAW
& CULBERTSON LLP

GOVERNMENT HEALTH IT

August 30, 2013

Commentary: The case for extending MU Stage 2

James M. Hofert, Partner, Hinshaw & Culbertson LLP and **Roy M. Bossen,** Partner, Hinshaw & Culbertson LLP and **Linnea L Schramm,** Associate, Hinshaw & Culbertson LLP and **Michael A. Dowell,** Partner, Hinshaw & Culbertson LLP and **David H. Levitt,** Partner, Hinshaw & Culbertson LLP

Healthcare-industry stakeholders — including associations, vendors, practitioners and providers — have raised two major concerns relating to implementation of Stage 2 and 3 meaningful use criteria: problems with interoperability and a regulatory failure to assess value added from implementation of meaningful use criteria to date.

The American Medical Association (AMA) recommended the creation of a public-private partnership that would include those stakeholders and the government to develop consensus standards that could be adopted broadly across the healthcare system concerning the design and implementation of electronic health records (EHR) systems to ensure interoperability. Stakeholders have also expressed concerns about the government regulatory failure to fund and conduct an independent comprehensive external progress evaluation of the meaningful use program to date and the adoption of incentives to encourage industry assessment of successes or failures in implementation. Additionally, they have expressed concern that individual providers are so involved in the adoption of technology that little effort is being directed toward assessment of whether care, quality and efficiency have been enhanced.

HIT was intended to establish an informational backbone for accountable care, and for patient safety and healthcare reform. Stage 1 of the meaningful use guidelines was intended to promote EHR adoption and infrastructure development. Unfortunately, it was not designed with sufficient forethought so as to require that design implementation and evolution of existing systems and infrastructure meet the goals of Stages 2 and 3. While Stage 1 barely scratched the surface of interoperability, Stage 2 requirements include stiff criteria in this area. Under Stage 2 rules, which take effect next year, healthcare organizations must provide a summary-of-care record in at least 50 percent of transactions and referrals, with a portion of those communications occurring between certified EHRs or indirectly through health information exchange. The two goals of HIT have always been the interoperability and usability of EHR systems that allow secure and responsible information exchange.

While commentators have expressed concerns about HITECH implementation for many years, original research by various respected medical organizations was published earlier this year on successes and challenges that have come to light from the implementation of HITECH, as perceived by the medical community. Concerns relate to the failure of the Office of the National Coordinator for Health Information Technology (ONC) to emphasize the need for interoperability in the implementation of Stage 1 requirements, resulting in the design, marketing and sale of EHR systems that cannot talk to each other; a lack of vendor regulation and oversight to ensure the design and sale of compatible systems, usability, and the lack of a means to ensure ongoing assessment of the implementation of EHR systems.

Difficulty in the perceived ease of use reflects widespread criticism of the usability of these tools. While ONC is making progress in this area, significant progress must be made before such systems are perceived to be usable by most physicians. Using EHR as a simple replacement for paper records will not result in the gains in quality and efficiency or reduction in cost that EHR has the potential to achieve.

The American College of Physicians (ACP) recently published original research on the effect of EHR on healthcare costs. The ACP noted that empirical evidence has not yet resolved the question of whether EHR will result in lower healthcare costs but that EHR use has resulted in strong savings in certain areas of medicine, such as radiology. The authors appear to express cautious optimism that EHR will produce true savings.

Presently, more than 700 vendors produce approximately 1,750 distinct certified EHR products. This certification, however, has historically not been focused on the ultimate goals of meaningful use.

The exploding electronic records industry is largely unregulated. Notwithstanding this growth, a few companies control much of the market and remain entrenched in legacy approaches. The lack of progress relating to interoperability has led some to speculate that major IT vendors are opposed to this goal.Commercial contracts between users and vendors often prohibit frank discussion about problems with a given system even in published medical literature. Concern also exists that such discussion of problems with EHRs may lead to malpractice lawsuits against the healthcare provider or product liability lawsuits against vendors. These communications are clearly not adequately protected from the legal community at this time.

Many have commented that although HIT use has increased, the quality and efficiency of patient care has, at best, improved only marginally. Others have suggested that EHR adoption has resulted in medical errors, causing harm and even death. Worse yet, annual aggregate expenditures on healthcare have increased from approximately $2 trillion dollars in 2005 to $2.8 trillion dollars in 2013, a far cry from the rosy future that HIT supporters promised.

Despite governmental encouragement to increase interoperability among HIT systems, ONC reported last year that only 19 percent of hos-

pitals suggested successful exchange of clinical information electronically with providers outside their system.

A major reason for the low level of interoperability, according to ONC, was the expense of interconnecting disparate EHR systems. No one state or organization has sufficient influence over the community of vendors to reduce design variability in available EHR systems. While national interoperability standards have recently been published, regulation and enforcement remains an issue.

Because of the shortcomings in the design and implementation of HIT systems, many providers are reluctant to invest the considerable time and effort required to master difficult user technology and to implement process changes required to fully realize HIT potential. The most recent data available suggests that only about 27 percent of hospitals are using basic EHR. Fear of rapid obsolescence and uncertainty about the future regulatory environment are cited as reasons for delay in HIT adoption. While there has been convincing evidence that federal incentives have accelerated HIT adoption, most of this adoption has been among providers that had already planned improvements in this area, as opposed to small, rural and nonteaching institutions.

This can also be partly attributed to a failure to deliver quantifiable gains in productivity and patient safety and may, in part, be due to a failure to engage doctors and healthcare providers early in the HIT development process.

Several specialty groups (emergency room physicians and pediatricians) have noted that usability issues impair the advancement of EHR use in the healthcare community. System functionality varies greatly and affects physician decision making, clinical workflow, communication and, ultimately, the overall quality of care and patient safety. EHR safety concerns arising from use of inferior EHR products or suboptimal execution of such products in the clinical environment include: (a) communication failure; (b) wrong order/wrong patient errors; (c) poor data display; and (d) alert fatigue. As HIT products become more intimately involved in the delivery of care, the potential for HIT-induced medical errors causing harm or death has increased significantly. Authors have cited dosing errors, delays in diagnosis and delays in treatment issues because of poor human-computer interaction or loss of data as HIT evolves. EHR errors are often attributed to user experience level and training but may occur due to human errors secondary to poor design of products.

Usability concerns include violation of common interface design, heuristic rules such as presenting consisting models of function or usable, legible workflow mismatching related to lack of consistency between provider modeling of work, and design models inscribed into EHR. Deficiencies in IT system designs can inhibit provider discovery of error and efforts to correct such error.

Problems in the implementation of meaningful use standards to ensure usability and interoperability to promote the goals of HITECH have plagued the healthcare system. These issues arguably have contributed to a failure of the majority of healthcare providers and institutions to adopt EHR designed to meet Stages 1 and 2 meaningful use criteria. Design evolution to meet existing use criteria by 2014 is further impeded by the reticence of stakeholders and vendors to exchange information on successes and failures in the implementation of EHR systems. The industry and regulators have started to confront roadblocks adversely affecting the evolution of the program. However, these efforts have historically neither been adequately planned nor coordinated to ensure success.

ONC should consider delay in implementation of Stage 2 and 3 criteria pending implementation of controls to ensure interoperability and usability, as well as measures to honestly evaluate progress in a systematic way to ensure cost efficiencies and improved care.