Healthcare fraud is growing at an increasing and alarming rate. The National Health Care Anti-Fraud Association estimates that, “of the nation’s annual healthcare outlay, at least 3 percent, or $51 billion in calendar year 2003, was lost to outright fraud.” Other estimates by government and law enforcement agencies place the loss as high as 10 percent of our annual expenditure, or $170 billion.2 U.S. healthcare spending grew 7.4 percent in 2005 to surpass $2 trillion and is expected to grow 7.3 percent in 2006, the CMS said in an annual report. That is down from a
recent peak of 9.1 percent growth in 2002. The 7.9 percent increase in spending on hospital services outpaced overall healthcare spending growth for the second year in a row. CMS said Medicare spending will exceed $790 billion in 2015, up from $309 billion in 2004. Medicaid spending, meanwhile, will hit $670 billion in 2015, up from $293 billion in 2004.3

The amount of money lost to fraud and abuse for 2006 is estimated to be $48 billion to $80 billion. That estimate of annual healthcare spending wasted through fraud is based on the calculation that 3 percent to 5 percent of all healthcare spending is lost to fraud, according to the National Health Care Anti-Fraud Association.4

As healthcare expenditures rise, so does the opportunity for fraud to escalate. The growing number of claims processed electronically and over the Internet has dramatically improved processing efficiency and reduced the processing cycle from days and weeks to hours and minutes. These changes have increased the potential for large sums of money to change hands very quickly, and they also have increased the exposure for losing large sums of money.

The National Health Care Anti-Fraud Association defines fraud as “the deliberate submittal of false claims to private health insurance plans or tax-funded health insurance programs, such as Medicare and Medicaid.”5

“As healthcare expenditures rise, so does the opportunity for fraud to escalate.”

The problem of fraud and abuse within the healthcare system comes from two sources: providers and patients. A provider is anyone who is authorized to give care by the Secretary of the Department of Labor.6

The types of provider fraud are numerous and vary in magnitude. Provider fraud and abuse includes:

- Multiple billing or billing for procedures that are unnecessary or not rendered.
- Falsely stating a condition or diagnosis of a patient to justify unnecessary and sometimes costly tests.
- Submitting a bill for services that cost more than what was actually provided, also known as upcoding.
- Submitting separate bills for each phase of a procedure, also called unbundling.
- Sharing a single patient ID to create billings for multiple providers, also known as ping-ponging.
- Receiving a monetary reward for referring a patient, also known as a kickback.
- Encouraging individuals to go to clinics for unnecessary procedures or buying the health insurance information of unsuspecting citizens for fraudulent billing purposes, according to the State of Connecticut’s Insurance Department, which defines a scheme that has been emerging in healthcare fraud known as “rent-a-patient.”
- Hospitals holding a patient in observation status, which tends to reimburse at a higher cost, rather than admitting them as a patient.
- Durable medical equipment suppliers charging insurance providers for a different, more expensive equipment model rather than what was actually given to the patient.
- DME suppliers offering to pay patients for their Medicare number.
- Ambulance services billing for more miles than what they actually drove.

Patients also can perpetrate fraud in healthcare. Examples of patient fraud and abuse include:

- Using another person’s insurance card.
- Providing a name of an ineligible person to receive coverage.
- Submitting claims for nonexistent services or medications.
- Falsifying bills or receipts.

The reason fraud continues to run rampant—the bulk of it being undetected—is that the industry’s detection and control systems are not aimed at criminal fraud. The ‘edits’ and audits built into modern, highly automated claims-processing systems are designed with honest providers in mind and serve the purpose of catching errors, testing eligibility, matching diagnoses to procedure codes, checking pricing and, if necessary, sending claims back for correction.7

But the system enables criminals, intent on stealing millions as fast as possible, to have an easy time. All they have to do is aim their claims smack in the center of medical orthodoxy and policy coverage, and they can rest assured that automated systems will process their payments at the speed of light, with no human involvement at all, a process called auto-adjudication. In other words, to beat all the industry’s current defenses, all they have to do is bill correctly. If they do that correctly, they are free to lie.8

Contrary to popular belief, the principal vulnerability of large automated payment systems is not unauthorized intrusion, or “hacking.” Rather, the major worry is that these systems will work perfectly, quickly, and efficiently, time after time, but paying incoming claims that are false. The surprising motto for high-tech healthcare fraud is that fraud works best when processing systems work perfectly.9

Healthcare fraud management is more of an imperative by the federal prioritization of a NHIN. Interoperable EHRs on the NHIN and any regional health information organization will provide opportunities to access clinical information, not only payment information. The prospect of a NHIN that is interoperable with any RHIO creates new challenges and new opportunities for fraud management. However, there is
a tremendous potential to reduce healthcare fraud using a nationwide health information network and RHIOs with interoperable EHRs.

**RHIO and NHIN Definitions**

A regional health information organization is a group of organizations with a business stake in improving the quality, safety, and efficiency of care delivery. The purpose of a RHIO is to electronically exchange health information in a secure format so the receiver can use the information. The terms RHIO and health information exchange, or HIE, are often used interchangeably.

A health information exchange is the mobilization of healthcare information electronically across organizations within a region or community. A HIE provides the capability to electronically move clinical information between disparate healthcare information systems while maintaining the meaning of the information being exchanged. The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, and equitable patient-centered care.

*The reason fraud continues to run rampant—the bulk of it being undetected—is that the industry’s detection and control systems are not aimed at criminal fraud.*

Formal organizations now are emerging to provide both form and function for health information exchange efforts. These RHIOs are ordinarily geographically defined entities that develop and manage a set of contractual conventions and terms, arrange for the means of electronic exchange of information, and develop and maintain HIE standards.

Although HIE initiatives differ in many ways, survey results and experiences with states, regions, and communities indicate that those who are experiencing the most success share certain characteristics. Successful initiatives are governed by a diverse and broad set of community stakeholders; develop and assure adherence to a common set of principles and standards for the technical and policy aspects of information sharing; develop and implement a technical infrastructure based on national standards to facilitate interoperability; develop and maintain a model for sustainability that aligns the costs with the benefits related to HIE; and use metrics to measure performance from the perspective of: patient care, public health, provider value, and economic value.

ONC provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of healthcare and the ability of consumers to manage their care and safety. The first step taken by ONC was to foster regional collaborations among healthcare entities so a patient’s information can be securely stored in the local community and be electronically accessible to those involved in providing care in that community.

RHIOs today vary in the ways they approach data sharing, and most cannot communicate patient information outside their own system. As momentum builds and more RHIOs or HIEs are formed, a common approach for their development is needed to support the overall goal of healthcare data exchange among them.

Local RHIOs must be able to use a common set of standards so they can communicate with one another. Interconnecting each RHIO will require an infrastructure, known as the nationwide health information network, to facilitate interoperability among RHIOs. This will enable medical information to travel anywhere with patients, thus revolutionizing the industry by making information more consumer-centric. HHS proposed convening a private-sector consortium to plan, develop, and operate the NHIN.

The NHIN will be a nationwide utility or public infrastructure that links disparate healthcare information systems together to enable patients, physicians, hospitals, public health agencies, and other authorized users across the nation to share clinical information in real time under stringent security, privacy, and other protections.

In November 2005, HHS Secretary Mike Leavitt announced the award of contracts totaling $18.6 million to four groups of healthcare and health information technology organizations to develop prototypes for NHIN architecture. The expectation is that these four consortia will move the nation toward the President’s goal of personal electronic health records by creating a uniform architecture for healthcare information that can follow consumers throughout their lives.

“The Nationwide Health Information Network contracts will bring together technology developers with doctors and hospitals to create innovative state-of-the-art ideas for how health information can be securely shared,” Secretary Leavitt said. “This effort will help design an information network that will transform our healthcare system resulting in higher quality, lower costs, less hassle, and better care for American consumers.”

These contracts complete the foundation for an interoperable, standards-based network for the secure exchange of healthcare information. HHS previously has awarded contracts to create processes to harmonize health information standards, develop criteria to certify and evaluate health IT products, and develop solutions to address variations in business policies and state laws that affect privacy and security practices that may pose challenges to the secure communication of health information.
Increasing Anti-Fraud Activities

In June 2005, the ONC contracted with the FORE of AHIMA to conduct a research project to assess the use of health information technology to potentially expand or enhance healthcare anti-fraud activities. The project’s primary objective was to identify best practices that would enhance the capabilities of a nationwide interoperable health information technology infrastructure to assist in healthcare fraud prevention, detection, and prosecution. The field-based research was directed at studying emerging and rapidly evolving information technology and policy.

The principal research question for the economic framework is, “What are the expected fraud and non-fraud related costs and benefits associated with developing and implementing an NHIN with interoperable EHRs?”

The model examined four states through which the NHIN will evolve:

1. **The status quo.** This stage is anticipated to occur in 2006 after implementation of the Medicare Part D prescription benefit. In this stage, there is no NHIN. Some EHRs and electronic transactions such as e-prescribing exist, but, with the exception of claims and prescription databases, there is little aggregate clinical data and no interoperability.

2. **Early NHIN.** In this state, electronic clinical transactions such as laboratory results and e-prescribing become widespread. EHR adoption increases, but there is little EHR interoperability among providers.

3. **Intermediate NHIN.** This stage features interoperability with intelligent coding tools. A record locator system exists to facilitate the interchange of clinical records among providers. Clinical vocabularies are in widespread use, ICD-10 has been implemented and intelligent coding tools are used for claims generation.

4. **Advanced NHIN.** This state features advanced analytics. Interoperability enables the aggregation of rich clinical and financial databases to which advanced analytic techniques are applied to detect patterns of fraud.

Major Research Findings

“Fraud” in the healthcare context is defined by a number of legal authorities, but all definitions have common elements: a false representation of fact or a failure to disclose a fact that is material to a healthcare transaction, along with some damage to another party that reasonably relies on the misrepresentation or failure to disclose.

The healthcare fraud problem is a serious and growing nationwide crime, linked directly to the nation’s ever-increasing annual healthcare outlay. Healthcare fraud is a significant drain on the nation’s healthcare system, and there is a tremendous potential to reduce healthcare fraud and achieve substantial financial benefits using a nationwide health information network with interoperable EHRs.

Technology can play a critical role in detecting fraud and abuse and can help to pave the way toward prevention. While technology cannot eliminate the fraud problem, it can significantly minimize fraud and abuse and ultimately reduce healthcare fraud losses. The use of advanced analytics software built into the NHIN is critical to fraud loss reduction.

Information available via the NHIN must comply with all federal and state laws. The federal government continues to expand its initiatives to uncover healthcare fraud, waste, and abuse. It is important that healthcare organizations have an effective compliance program in place. It is particularly important to develop a corporate culture that fosters ethical behavior. Many healthcare organizations are developing such a corporate culture through the adoption of corporate compliance programs.

There is no single definition of the legal health record across the country. There is also no definition that encompasses the more complex electronic environment and various hybrid situations between paper and electronic records.

Moving to interoperability in the intermediate NHIN economic state may provide the most dramatic improvement in fraud in terms of net costs and benefits. The economic model demonstrates that there may be substantial savings in fraud-related expenditures that are possible from a move to an intermediate NHIN that are not realized in the status quo and early NHIN states.

Next Steps for HIT Leadership

The first step was the healthcare IT vision provided by President Bush and the ONC. The HIT leadership is actively moving forward to establish the foundation to meet the vision.

It is essential to develop the NHIN infrastructure to enable healthcare fraud management as part of its initial design. The design needs to establish the advanced NHIN state identified in this research as its ultimate endpoint. The advanced NHIN features advanced data analytics. Interoperability enables the aggregation of rich clinical and financial databases to which advanced analytic techniques are applied to detect patterns of fraud. It is when we have a comprehensive NHIN with interoperable RHIOs or HIEs, that the ongoing evaluation of data and the ability to identify fraud patterns will be achieved.

Designing fraud management functionality into the NHIN has the potential to significantly reduce healthcare fraud losses, and interoperability between multiple EHRs is a major enabler of these loss reductions. Maximum benefit will be achieved by linking a claim with its corresponding clinical documentation from an EHR. Having the ability to access information in other EHRs regarding the same patient, and applying advanced analytics to aggregate clinical and financial databases, will enable predictive modeling of data. Without a deliberate effort to build fraud management into the NHIN, healthcare payers and consumers will be exposed...
to new and potentially increased vulnerability to electronically enabled healthcare fraud.

ONC will begin a research effort to support the evolution and maturation of RHIOs. The initiative was announced in February 2006 by David Brailer, MD, PhD, then national coordinator for health information technology, at the opening keynote address at the 2006 Annual HIMSS Conference & Exhibition in San Diego. The research will ensure that RHIOs have a minimum set of functional capabilities, discern best practices among these organizations, and help organizations benefit from those best practices.

"While technology cannot eliminate the fraud problem, it can significantly minimize fraud and abuse and ultimately reduce healthcare fraud losses."

An important next step in 2006 is for the aforementioned RHIO research and for the American Health Information Community to consider and act on the findings of this research and to begin the necessary efforts to prevent, detect, and prosecute healthcare fraud.

At a minimum, the next steps should be to define a single definition of the legal health record across the country; define the infrastructure components that must support the legal health record for both patient care and as admissible evidence in fraud management; define the standards for EHR process and data standards that both facilitate fraud management and prevent abusive or fraudulent behaviors; adopt national metrics for healthcare fraud management to systematically gauge and reduce healthcare fraud; and raise awareness of the importance of coordinated fraud management across all stakeholders.

The healthcare industry has much to learn from the U.S. financial industry. The banking industry’s transformation from paper-based information to electronic information began 15 years ago, when banking began addressing the inefficiencies of paper. Eight years ago, federal mandate opened up interstate banking laws and ushered in the IT era for banking.

It has taken banking eight years to achieve a 51 percent rate of checks being electronic instead of paper. Banking made a huge investment in technology early to achieve efficiencies and fraud reduction. The banking industry required a national, uniform, standard coding system for banking transactions. The Banking Administration Institute was created and made responsible for maintenance of quality standards and codes. Every standard bank transaction has an industry standard BAI code that enables data sharing and that is used to detect fraud via advanced analytics software. The banking industry can provide the lessons that will enable the healthcare industry to move forward.

Recommendations for RHIOs

The conventional thinking is that the adoption of EHRs and participation in an interoperable RHIO, HIE, or NHIN will be voluntary and not mandated. While there are many understandable reasons for such assumptions, it is also apparent that those who are the most aggressive perpetrators of fraud almost certainly will opt out of the NHIN to avoid its anti-fraud capabilities.

Thus, the architects of RHIOs, along with NHIN, and those involved with payment systems may want to consider the advantages and disadvantages of a system that, at some point in the future, might predicate payment of claims on participation in the NHIN, assuming of course that this becomes feasible technologically and economically. While that would certainly increase the anti-fraud potential of the NHIN, strong consideration must be given to the fact that this might seem unduly coercive and could mandate significant added costs for certain providers.

National metrics for fraud management are required to systematically gauge and reduce healthcare fraud. Public and private stakeholder collaboration, as well as interstate cooperation, is required to fight healthcare fraud. Such an anti-fraud enabled RHIO or NHIN has the potential to identify emerging fraud schemes before payment. A shift from the current “pay and chase” fraud management programs to the proactive prevention of fraudulent claims before payment is made possible by interoperable EHRs coupled with automated fraud detection and advanced analytics software.

Typically, sophisticated applications to detect fraud and abuse are based on one or more of the following algorithms.

- Rules-based expert systems implement the thought process a human investigator would use. A rules-based fraud detection application includes a number of known rules based on historical behavior. Better expert systems enable the addition of new rules as investigators uncover new schemes.
- Neural networks enable the fraud detection application to “learn” rules based on the data. These types of systems are used in pattern-recognition systems to look for aberrations in claims.
- Predictive modeling uses historical and new data to predict behaviors. This technique can be implemented using regression techniques, decision trees, clustering, rules, and neural networks.
- Data mining is used to find relationships and makes forecasts. Data mining algorithm categories include clustering, which enables the discovery of unknown groupings in the data; association, which can identify new relationships and rules; sequential patterns, which are used to
FOCUS: Integration and Interoperability

anticipate behavior patterns and trends; classification algorithms, which involve various methods of grouping data; neural networks, which involve non-linear predictive models that learn through training; and predictive algorithms, which are time sequences that can reveal examples of similar fluctuations over a period of time.

The eHealth Initiative and its foundation is seeking to answer many of the questions that surround information exchange with the release of its Connecting Communities Toolkit, a “playbook” of principles and tools designed to equip local communities with the information and expertise to begin or advance local HIE organizations.

For the past three years, the eHealth Initiative has been assisting communities in their efforts to connect the HIE dots. The eHealth Initiative and its foundation are independent not-for-profit affiliated organizations that bring together multiple diverse stakeholders to improve the quality, safety, and efficiency of healthcare through information and information technology.20

As RHIOs and HIE communities follow the guidelines of

Preamble
The principles are based on a solid understanding of the vulnerabilities of the system to individuals with the intent to defraud and of the opportunities that well-designed health IT offers. They are intended to guide policy makers and to support the needs of the vast majority of providers of services who are striving to comply with honesty to laws and requirements that affect billing and reimbursement. While many of the recommendations cannot currently be implemented, they identify the future technology, capability, and capacity that will be needed.

Guiding Principles

1. The Nationwide Health Information Network (NHIN) policies, procedures, and standards must proactively prevent, detect, and support prosecution of healthcare fraud rather than be neutral to it.
2. EHRs and information available through the NHIN must fully comply with applicable federal and state laws and meet the requirements for reliability and admissibility of evidence.
3. A standard minimum definition of a Legal Health Record (LHR) must be adopted for electronic health records (EHRs).
5. Healthcare Fraud Management is the responsibility of all healthcare stakeholders.
6. Increased consumer awareness of healthcare fraud and the role health information technology and EHRs play in its reduction can improve the effectiveness of healthcare fraud management programs.
7. EHR standards must define requirements to promote fraud management and minimize opportunities for fraud and abuse, consistent with the use of EHRs for patient care.
8. Standardized reference terminology and up to date classification systems that facilitate the automation of clinical coding are essential to the adoption of interoperable EHRs and the associated IT enabled healthcare fraud management programs.
9. Fully integrate and implement fraud management programs and advanced analytics software in interoperable EHRs and the NHIN to achieve all of the estimated potential economic benefits.
10. Data required from the NHIN for monitoring fraud and abuse must be derived from its operations and not require additional data transactions.

Table 1. Health Care Fraud Management Guiding Principles21
the eHealth Initiative Toolkit and the direction of AHIC, ONC, and other HIT leadership, the guiding principles (see Table 1) created through the anti-fraud research should be incorporated into each organization’s fabric.

Summary
Organizations must accept the fact that fraud is not a competitive issue. All organizations must work together to develop, collaborate, and harmonize data standards.

Substantial savings in fraud-related expenditures would be enabled by an NHIN. However, it is important to move quickly through the early transition state of the NHIN and achieve widespread adoption to maximize net savings.

Remember, conservative estimates indicate that “of the nation’s annual healthcare outlay, at least 3 percent, or $51 billion in calendar year 2003, was lost to outright fraud. Other estimates by government and law enforcement agencies place the loss as high as 10 percent of our annual expenditure, or $170 billion.” This number will continue to grow exponentially without an interoperable system of EHRs, RHIOs, and NHIN. Without data standards and interoperability, the obsolete but nonetheless existing pay-and-chase method of fraud control will be the only option.

The only option for the United States healthcare industry is to follow the model of the banking industry and build an interoperable network of RHIOs, HIEs, and have a fully functioning NHIN with fraud management built into the design.

Acknowledgments
The authors would like to thank FORE/AHIMA and the Office of the National Coordinator for Health Information Technology for their assistance.

About the Authors
Susan P. Hanson, MBA, RHIA, FAHIMA, is president of TerraStar Consulting in Nashua, N.H.

Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS, is president of Cassidy & Associates in Peachtree Corners, Ga.

References
8. Ibid.
9. Ibid.
14. Ibid.
17. Ibid.
18. http://www.hhs.gov/healthit/ahic.html. The Community is a federally chartered commission and will provide input and recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way.
FOCUS: Integration and Interoperability

20. Health Leaders Extra; eHealth Initiative Launches Interactive Application to Aid Community Health Information Exchange; by Katherine H Capps and Sandy Mau, for Health Leaders News, February 24, 2006.

21. Each of the guiding principles has accompanying recommendations which can be found in the executive summary of the “FORE/ONC Report on the Use of Health Information Technology to Enhance and Expand Health Care Anti-Fraud Activities,” found on at http://www.hhs.gov/healthit/hitca.html.


Congratulations CPHIMS Recipients!

Congratulations to the following individuals who recently achieved the Certified Professional in Healthcare Information and Management Systems (CPHIMS) credential from October 17, 2005, through March 31, 2006. The CPHIMS designation is recognized throughout the industry as a national standard of industry knowledge. The designation is an indication that an individual has met the eligibility requirements and passed the CPHIMS examination, demonstrating to superiors, colleagues, and potential employers their dedication to the industry, dedication to high standards, and pride in their own professionalism.

Frederick L. Banner—Somers Point, NJ
Gary L. Barnes—Odeessa, TX
Scott E. Bateman—Norfolk, VA
Judith S. Best—Saint Petersburg, FL
Claudia M. Blackburn—Baton Rouge, LA
Gordon D. Bradberry—Ogden, UT
Robert Brandner—West Hartford, CT
Melvin J. Brewster—Altadena, CA
Rodney J. Burns—Brampton, Ontario, Canada
Robert G. Burritt—Dayton, OH
Thomas P. Carrico—Lexington, KY
Kathleen G. Charters—Columbia, MD
Barbara K. Coulter—Beech Grove, IN
Egbert H. Creque, Jr.—St. Thomas, U.S. Virgin Islands
St. Thomas, U.S. Virgin Islands
Glynda Crunk—Newnan, GA
Daniel K. Cumberland—Washington, DC
Thomas K. Cutler—Corinth, TX
Cheryl L. Daffron—Wichita, KS
Kimberly A. Deese—New Braunfels, TX
Susan A. Demorsky—Frisco, TX
Stacie DePau—Yucaipa, CA
Gary R. Eckel—Cleveland, TN
John C. Eckmann—Titusville, FL
Michael J. Gomez—Grosse Pointe, MI
Dane Gregor—Tampa, FL
Thomas H. Gregorich—Cleveland, OH
Margaret O. Griscom—Stone Mountain, GA
James P. Haggard—Pasadena, CA
Jim S. Hahn—Palo Alto, CA
Adnan E. Hamid—Pasadena, CA
Janet F. Harvey—Seattle, WA
Todd C. Hatton—Kansas City, MO
W. Glenn Hilburn—Atlanta, GA
Michael R. Jones—Baltimore, MD
John P. Kansky—Indianapolis, IN
Janet D. Kasoff—Arlsby, NY
Bruce K. Kelly—Poniatci, MI
Charles Kennedy—Santa Rosa, CA
Todd D. Klein—League City, TX
Kevin E. Kujawa—San Diego, CA
Gil E. Lalo—Grand Rapids, MI
Randy Lane—Tucson, AZ
Cynthia D. Leed—Red Bank, NJ
Jacqueline P. Littlejohn—Jacksonville, FL
John C. Mahby—Draper, UT
Mary B. Mars—Naperville, IL
Kelly P. Martin—Seattle, WA
Nancy E. McCarr—Halifax, Nova Scotia, Canada
Theresa Z. Meadows—Birmingham, MI
Frank W. Meisner—Del Rio, TX
Susan M. Mehlsheimer—Baton Rouge, LA
Jaclyn A. Miller—San Diego, CA
Mary L. Moewe—Nashville, TN
Robert L. Mori—Dallas, TX
Andrew R. Needleman—Newton, MA
Margaret K. Neidlinger—Baltimore, MD
Christopher C. O’Connor—Wilmington, DE
Tina M. Oleskiai—Mayfield Heights, OH
Ketan P. Palucha—Novi, MI
Patrick K. Pearsy—North Charleston, SC
Susan E. Peters—Annandale, VA
Chekuri V. Rauji—Farmington, MI
Linda M. Reeder—Seattle, WA
Janice E. Rester—Birmingham, AL
Michael S. Rester—Mountain Brook, AL
Harry B. Rhodes—Mokena, IL
Timothy D. Rice—Saint Louis, MO
Chris D. Rih—Roanoke, VA
Jason L. Roberts—Fort Jackson, SC
James M. Roling—Cincinnati, OH
Jason E. Roos—Houston, TX
Marilyn Rugh—Albany, NY
William Sgriccia—Ann Arbor, MI
Daniel R. Shoemaker—Morris, IL
Michael A. Short—Waverly, TN
Renfa L. Simpson—Fort Lauderdale, FL
Paul M. Siva—Des Moines, IA
David H. Snyder—Albany, NY
Joseph F. Speroni—Albuquerque, NM
Robert S. Strickland—Birmingham, AL
Diana K. Stump—Aurora, IL
Brian L. Taylor—Ashland, KY
Laura S. Tillery—Potomac, MD
Lisa S. Trask—Sacramento, CA
Robert J. Turk, Jr.—Wadsworth, OH
Grace M. Upleger—Nashville, TN
B. Alex Vaillancourt—Oxford, OH
Arthur M. Vincent—Atlanta, GA
Jane H. West—Walnut Creek, CA
Joshua W. Wharton—Red Bank, NJ
John H. Wright—Newport Beach, CA
Russell A. Yeager—Birmingham, AL
Richard W. Znidarsic—Dewitt, MI

Join this elite group. Go to www.himss.org/getcertified to find out more about the CPHIMS certification program. To see a full listing of certificants go to http://www.himss.org/content/files/cphims_certificants.pdf.