AHIMA CONFERENCE **DIGITAL SUPPLEMENT**

FOR THE RecorD

ICD-10 CODING SUCCESS: The Devil Is in the Details

PCS codes present unique challenges.

What's INSIDE

AHIMA—YOUR HIM RESOURCE!

AHIMA supplies all the tools necessary to help further your career and prepare for ICD-10 Implementation.

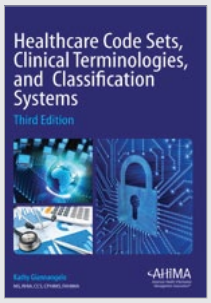
Resources include:

- Online training for physicians, coding, and non-coding professionals
- Industry-respected HIM, specialty, and coding credentials
- Books and publications
- Events, webinars, and seminars
- ICD-10 training academies

Attending AHIMA's 86th Convention and Exhibit in San Diego?

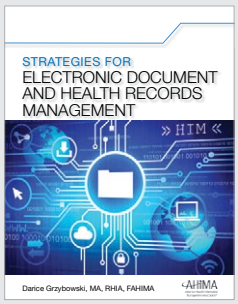
Visit the AHIMA Booth (#1943) and save with the onsite purchase of these and other publications.

NEW PUBLICATIONS



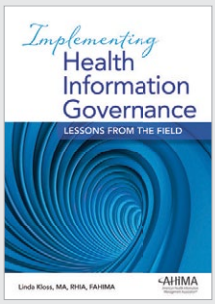
Healthcare Code Sets, Clinical Terminologies, and Classification Systems, Third Edition

Product #: AB201913
Price: $89.95
Member Price: $74.95



Strategies for Electronic Document and Health Record Management

Product #: AB113013
Price: $79.95
Member Price: $64.95



Implementing Health Information Governance: Lessons from the Field

Product #: AB100213
Price: $59.95
Member Price: $49.95

AVAILABLE FOR PRE-ORDER

ICD-9-CM Code Book, Volumes 1, 2 & 3, 2015 Ed.
Product #: AC242014 | Price: $110 | Member Price $89.95

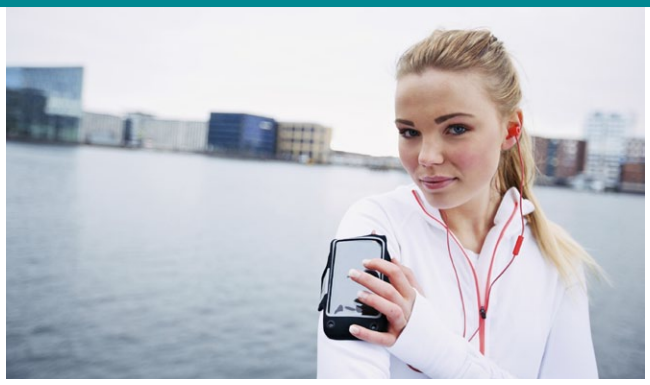
ICD-10-CM Coder Training Manual, 2015
Product #: AC216815 | Price: $99.95 | Member Price: $79.95

ICD-10-PCS Coder Training Manual, 2015
Product #: AC207815 | Price: $99.95 | Member Price: $79.95

For a complete list of available products and resources, visit ahima.org today!

AHIMA PRESS

MX9965



Data Avalanche Requires Context, Standards

By Vern Davenport

If properly managed, information culled from mobile devices can reshape health care.

In a 2013 ***Health Affairs*** policy briefing, the Robert Wood Johnson Foundation concluded that a growing body of evidence demonstrates that patients who are more actively involved in their health care experience better health outcomes and incur lower costs.[1]

It is perhaps, then, no surprise that a top priority for the vast majority of health system leaders nationwide is to boost patient engagement.[2] While patient engagement comes in many forms, one newer method currently exploding in popularity is patients using wearable devices or smartphone applications to monitor their physical fitness and other health behaviors. In fact, according to Juniper Research, the smart, wearable device market is expected to reach $19 billion by 2018, up from only $1.4 billion in 2013.[3]

As patients—who are quickly becoming health care consumers due to their increasing out-of-pocket responsibility and the Affordable Care Act's health coverage mandate—begin adopting these devices, they will demand their collected data be integrated with their medical records and available to their health care provider. Once these health care consumers depend on these products' offerings for daily use, a sense of "stickiness" will surround the use of each product. This stickiness will ensure the continued use of the product by consumers and in turn allow providers to obtain and analyze important data to achieve their Triple Aim goals of improving the patient experience, improving the health of populations, and reducing health care costs.

For the "sticky" technology to achieve these ends, however, three factors must be present. The first is the data from these devices and applications must be delivered in some meaningful context so the provider can easily understand them in a practical manner. The second is the technology must be mobile so the data can be captured anytime and anywhere for the sake of convenience and accuracy. The final factor is interoperability, which includes the ability for the consumer-captured data to be easily shared and universally understood across multiple systems.

Context Delivers Meaning and Drives Action

Hundreds of different health monitoring and fitness devices are bombarding hospitals and practices with a data avalanche that will not benefit any stakeholder unless the providers' backend information systems collecting that data present the information in a meaningful, evidence-based context to support decision making.

For example, a patient using a smart bodyweight scale wirelessly transmits his weight daily to his provider, exhibiting a steady weight gain over several days. These daily updates alone would likely be overlooked in a flood of other incoming data. However, if they are filtered through a clinical decision support engine that automatically accesses this patient's EHR and generates a notification for the provider that the patient is on a medication where sudden weight gain is a potentially dangerous side effect, then an intervention can be performed before an adverse event occurs. On the patient side, the smartphone application connected to the smart bodyweight scale also would be linked to the patient's medication list and would urge the patient to contact his provider as the weight gain is detected.

For healthy consumers not on a maintenance medication, the stickiness of a device or app will depend on its ability to deliver value so that they use the technology on a daily basis. Health systems and employers, which are very interested in ensuring these patients and employees maintain their healthy behaviors, should configure employer wellness programs to reward employees financially for achieving and reporting health and fitness metrics using a mobile device app. When the app shares consumer-supplied data, the health system would benefit by having a low-resource utilization consumer engaged in the system while the employee would appreciate an annual premium discount or other financial incentive from the employer.

Mobility Offers Convenience and Accuracy

Ensuring a health or fitness product's stickiness requires the device or app to deliver value to health care consumers, but it also must be convenient and simple to access and operate. As of January of this year, 68% of consumers own a smartphone, and of those mobile phone users who recently acquired a new device, 84% of those purchases were smartphones.[4] The increasing ubiquity of these devices means sticky consumer-facing health and fitness technology must be mobile and/or have smartphone integration capabilities.

This year, several major consumer electronics companies have announced agreements with health systems, HIT vendors, or other companies to partner on smartphone-based health and fitness monitoring applications and devices. These alignments indicate that industries besides health care are anticipating consumers will want to capture their own biometric data and share it with their providers using their smartphone or tablet as the bridge.

These entities realize mobile devices offer convenience, which encourages stickiness for the consumer, but the devices also increase the likelihood the data will be more accurate because the technology would automatically capture the information wherever and whenever it is required, either through sensors or software algorithms.

Interoperability Supports Trust

While automation will help reduce providers' skepticism of the data collected from these applications and devices, trust will continue to be a major hurdle for clinicians in the coming years. Increasing the use of standardized data formats, such as continuity of care documents (CCDs), will help with clinical adoption, but additional IT standards must be embraced by developers for their products to be truly valuable to the health care provider community. Standards like CCDs promote interoperability of systems, so when consumers want to share their blood pressure reading with their primary care physician, cardiologist, and endocrinologist, they will need to access only one application or device, ensuring stickiness. Likewise, providers, regardless of their EHR system or health system affiliation, would be able to automatically capture and add that reading to the relevant medical record because it was shared in a universally accepted technical and clinical format.

Prove Their Stickiness

In the near future, health systems and practices will be inundated with requests from the makers of consumer-facing devices and applications about integrating their technology with providers' information systems. While all of these companies will claim their products deliver valuable clinical data and support patient engagement, providers should demand these vendors prove their ability to perform on the three factors described above by answering the following questions:

1. Context: Can these vendors' technology deliver consumer-captured data in context using a decision-support engine that leverages evidence and EHR data?

2. Mobility: Can the device automatically capture data while the consumer is mobile and/or by linking to the consumer's smartphone or tablet?

3. Interoperability: Can consumers share their data in a universally accepted format that will be understood by the organization's information systems and by other providers across the care continuum?

If the answer to all three questions is yes, then the IT vendor is likely offering devices that will become a daily part of the lives of consumers. Stickiness alone, however, is only half of the engagement equation. Providers must integrate the technology and incorporate monitoring and analysis of consumer-captured data into their daily workflow so they can intervene when necessary. Even sticky technology is only a tool—it's up to the providers to leverage the solution to deliver high-quality care.

— Vern Davenport is president of Medfusion.

References

1. Health policy briefs: patient engagement. ***Health Affairs*** website. http://www.healthaffairs.org/healthpolicybriefs/brief.php?brief_id=86. Updated February 14, 2013.

2. Bird J. NeHC: Consumers engagement a must to transform healthcare. ***FierceHealthIT*** website. http://www.fiercehealthit.com/story/nehc-consumers-engagement-must-transform-healthcare/2013-10-11. Updated October 11, 2013.

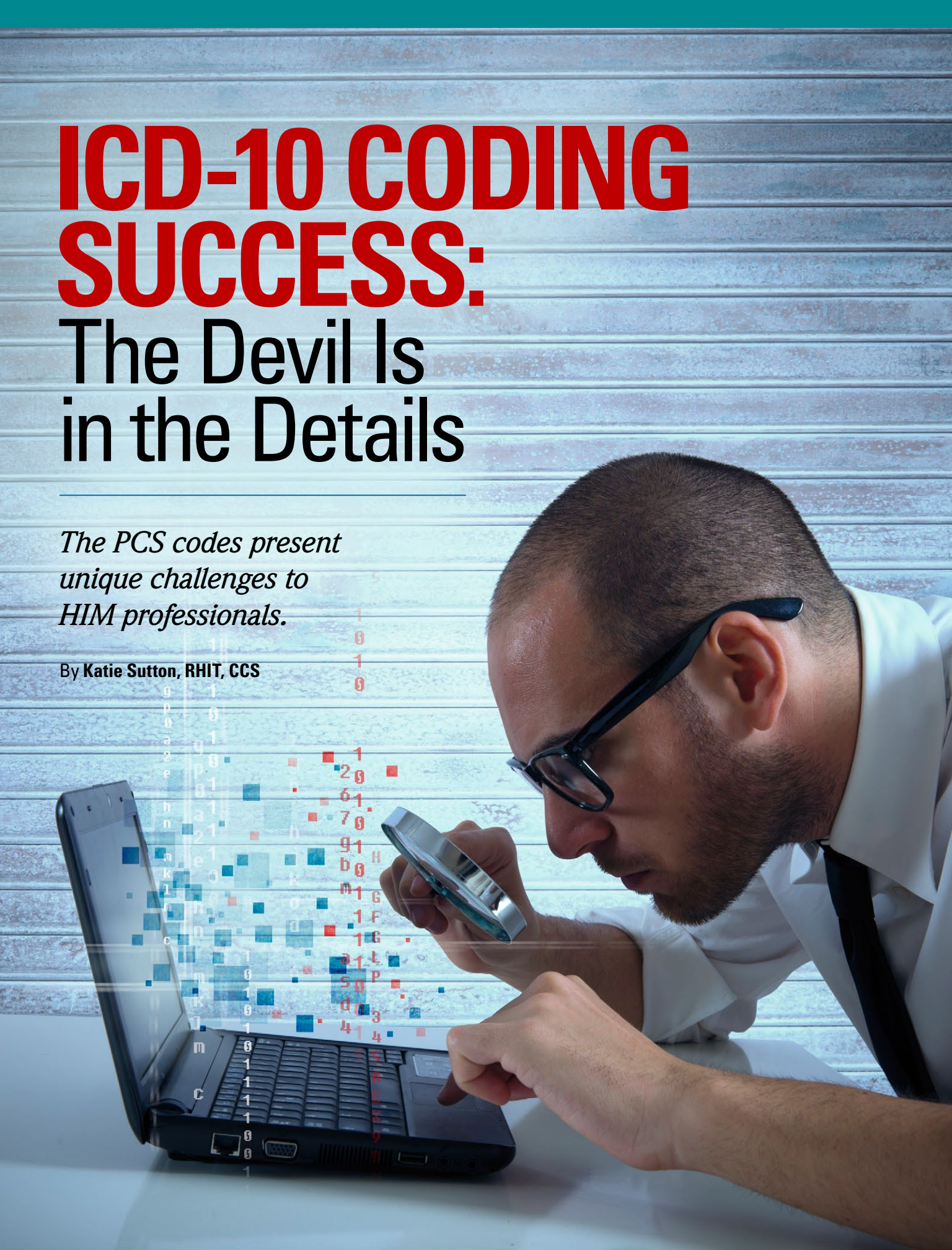
3. Press release: mobile smart wearable devices to be worth $19 billion by 2018, Juniper Research finds. Juniper Research website. http://www.juniperresearch.com/viewpressrelease.php?id=637&pr=405. Updated October 15, 2013.

4. Multiplying mobile: how multicultural consumers are leading smartphone adoption. Nielsen website. http://www.nielsen.com/content/corporate/us/en/insights/news/2014/multiplying-mobile-how-multicultural-consumers-are-leading-smartphone-adoption.html. Updated March 4, 2014.

ICD-10 CODING SUCCESS: The Devil Is in the Details

The PCS codes present unique challenges to HIM professionals.

By **Katie Sutton, RHIT, CCS**



ICD-10-PCS is a brave new world. The differences in terminology offer opportunities to broaden the outlook of patient care as well as notable challenges to HIM professionals. These realities are helping health care organizations develop a deeper awareness of what the broader scope of readiness really entails.

Accurate mapping strategies from ICD-9-CM to ICD-10 are a fundamental component of success. As health care organizations move into more advanced implementation stages, many are discovering that full conversion to ICD-10 will require the aid of industry crosswalks as well as customized mapping strategies. A gold standard tool that can address every use case simply does not exist in the industry today.

As part of a large project conducted by Health Language, our team embarked on a journey to provide a functional crosswalk between CPT-4 and ICD-10-PCS (PCS) codes that required the creation of more than 70,000 individual maps. This process allowed us to develop an intimate knowledge of potential problem areas for HIM professionals going forward when coding under PCS.

Below are some basics on the new system as well as a several key insights into potential pitfalls, key knowledge areas for HIM professionals, and best practice advice for being prepared.

ICD-10-PCS Basics

Scheduled for go-live on October 1, 2015, PCS is characterized by a multiaxial seven-character alphanumeric code structure that provides unique codes for procedures. PCS has key attributes that include the following:

- **Completeness:** It has a unique code for each substantially different procedure.
- **Expandability:** Its structure allows for easy expansion.
- **Multiaxial:** It contains independent characters and an individual axis that maintains its meaning across code ranges.
- **Standardized Terminology:** The definitions are well defined and eliminate multiple meanings by assigning each term a specific meaning.

The letters O and I are not used in PCS, but the numbers 0 and 1 are. Each character of the alphanumeric code has a meaning, which changes by sections.

Six Important Coding Considerations

1) There Are No Eponyms in PCS

Defined as a person after whom a discovery, invention, place, disease, or medical procedure is named, eponyms can be found for both diagnoses and procedures in the ICD-9-CM alpha index. All surgical eponyms have been removed from the content set of PCS and are now represented by root operations, which describe the objective of each procedure performed. Coders now will have to know the objective of a procedure, as well as how and to what extent it is being performed.

For example, a Whipple procedure is known as a pancreaticoduodenectomy. In ICD-9-CM, this procedure is coded to 52.7, radical pancreaticoduodenectomy, which includes all components of the procedure: the pancreaticojejunal anastomosis, choledochojejunal anastomosis, and gastrojejunostomy.

In ICD-10-PCS, the same procedure requires the assignment of the following five separate procedure codes:

- 0FBG0ZZ for the excision of the pancreas, open approach;
- 0DBA0ZZ for the excision of the jejunum, open approach;
- 0DB90ZZ for the excision of the duodenum, open approach;
- 0F1G0ZB for the bypass of the pancreas to the small intestine, open approach; and
- 0D160ZA for the bypass of the stomach to jejunum, open approach.

PCS more specificially defines an excision as cutting out or off, without replacement, a portion of a body part.

This new characterization supports better information sharing as the same eponym under ICD-9-CM may apply to more than one procedure, making it more difficult to paint a clear picture of patient care.

2) Excision vs Resection

Under ICD-9, an excision is a catch-all for a biopsy or removal of any part of the body. PCS more specifically defines an excision as cutting out or off, without replacement, a portion of a body part. Examples of excision procedures could include a partial nephrectomy or the removal of a malignant melanoma.

In cases where all of a body part is removed under PCS, procedures are classified as resections. Examples could include a total right-sided nephrectomy or a laparoscopic cholecystectomy.

3) Occlusion vs Restriction

Use of occlusion becomes more narrowly defined under PCS as completely closing an orifice or lumen of a tubular body part. Ligation of inferior vena cava and fallopian tube ligation (with bands, tied or cut) are appropriate examples.

In cases of gastric banding (lap band) or restriction of thoracic duct with intraluminal stent, restriction is the appropriate choice as these procedures are defined as partially closing an orifice or lumen of a tubular body part.

4) Revision vs Change

The use of revision also becomes more narrowly defined under PCS as correcting, to the extent possible, a portion of a malfunctioning device or the position of a displaced device. Under ICD-9-CM, use of "revision" is not tied to a device. Examples of appropriate uses are adjustment of a pacemaker lead or taking out a loose screw and replacing with a larger screw in a fracture repair.

A procedure is classified as a change if a device is removed from a body part and an identical or similar device is put back in or on the same body part without cutting or puncturing the skin or mucous membrane. Examples of appropriate uses under PCS include a urinary catheter change or exchange of a drainage tube from a joint.

HIM professionals must exercise caution when using revision because a complete redo of the original root operation is coded to the root operation and not to revision. If a coding professional is unsure of the root operation, the index and description of root operations must be referenced. Remember, PCS is new—it's OK to check and recheck.

5) Control vs Definitive Root Operation

Control, which is defined as stopping or attempting to stop postprocedural bleeding, is used to represent a small range of procedures. If another procedure with a definite root operation is performed to stop the bleeding, then control is not coded separately.

For example, resection of spleen to stop postprocedural bleeding is coded to resection instead of control.

6) Transplantation vs Transfusion

Under ICD-9-CM, transplantation refers to a living body part or blood. PCS separates the two procedures.

Transplantation is defined as putting in or on all or a portion of a living body part taken from another individual or animal to physically take the place and/or function of all or a portion of a similar body part. Kidney and heart transplants are appropriate examples.

In the case of blood products—bone marrow transplant or transfusion of cell saver red cells into a central venous line—"transfusion" is used.

Looking Forward

Preparation is the secret to success with ICD-10. Especially with PCS, HIM professionals will need to refresh their knowledge of anatomy, which is a major focal point of the new coding system.

Advanced terminology management solutions exist within the industry to provide the detailed customized mapping needed to succeed within the ICD-10 landscape. Laying a foundation of automation and leveraging a solid technological infrastructure can go a long way toward taking the guesswork out of the coding transition.

HIM managers must have a solid education strategy in place over the next year to prepare their staff members. Most importantly, HIM professionals need to practice, practice, practice.

— Katie Sutton, RHIT, CCS, is a clinical informatics manager with Health Language, part of Wolters Kluwer Health, and an ICD-10 approved trainer.

Do Your Printers and Copiers Pose a HIPAA Hazard?

By Kash Hatton and Nannette Sloan

It's true, making copies has privacy consequences.

Imagine that your hospital keeps getting served with malpractice claims by the same attorney. New plaintiffs every time; a new suit every few months. The lawyer somehow possesses surprisingly detailed information on your patients' cases. It's almost like he's looking directly into your medical records. Maybe he is. Maybe an employee is faxing him case files. Maybe he's culling the most promising ones and cold-calling the patients, inviting them to litigate.

You guessed it: this scenario really happened. It's just one way those innocent devices—fax machines, copiers, printers, scanners, and all-in-one multifunction devices (MFDs)—can create big headaches for health care providers.

Here's another example. A few years ago, CBS News purchased a copier previously used by a nonprofit health care plan and discovered private health information for up to 344,579 patients was visible on the hard drive. Who even knew copiers had hard drives? The health care plan ended up paying Health and Human Services (HHS) more than $1.2 million in damages for violating HIPAA privacy and security rules.

Smaller, unpunished, less sensational breaches occur around these devices every day. Let's face it—they blend into the office scenery. It's computers you should be worrying about, right? Although employees know to be discreet with patient information in their e-mails, conversations, and handwritten documents, they often overlook the privacy threat posed by their ostensibly benign, passive office printers.

What's the Danger?

First, there is the obvious matter of printed documents sitting in printer trays for anyone in the office to see or grab, purposefully or inadvertently. Then there's the information on the hard drive—yes, these devices do have hard drives. In fact, these devices are bona fide computers. Every scanned, copied, faxed, or printed document can leave a residual image on that hard drive.

Often these devices act as full-blown file servers containing documents, forms, and sensitive address books. They also are connected directly to an office or hospital network and the Internet, capable of sending anything they touch to anyone or anything on the planet. The newest and most powerful ones come with full-blown Web browsers and hosts of apps that invite users to route documents to "the cloud."

All of this power, embedded in these devices for very good reason, makes it easy for a health care organization to appear foolish or even negligent in the event of an audit by HHS' Office for Civil Rights (OCR), the agency responsible for enforcing HIPAA and HITECH regulations around heath information privacy, security, and breach notification. The government won't let you plead ignorance. HIPAA explicitly requires health care providers and business partners to implement administrative, physical, and technical safeguards to protect private electronic health information.

If you are audited, the OCR will want you to produce the following:

- evidence of policies and procedures aligning to the HITECH Act;
- a list of information systems, applications, and hardware;
- a description of encryption methods being used;
- organizational charts;
- security plans for your building and technical architecture, including authentication and access control;
- evidence of security and privacy training for all employees, including consultants;
- network diagrams; and
- evidence of business associate agreements.

The auditing process will take around 90 days from notification letter to final audit report, a process that will include document production, review, onsite field audit work, draft report review, commenting, and final report delivery. If deficiencies are noted, you could receive technical assistance, undergo extended compliance review, or, of course, face big penalties.

How to Avoid the Audit and Worse

Poor audit results are only a symptom of the main problem, which is that your patients' private health information may be in jeopardy. There also is the serious problem of jeopardizing your organization's reputation and, thus, the entire enterprise. No matter how long unsullied your brand may be, the stain of a breach could take years to remove.

Although the consequences can be serious, it is entirely realistic to head them off by taking a proactive look at your copier, printer, scanner, fax, and MFD environment in order to implement proper safeguards to ensure you have completed a risk assessment.

Physical Security

The following safeguards must be considered:

• **Make users prove their identity.** Require employees to swipe smart cards or at least key in PIN codes to operate devices. In addition to keeping unauthorized users at bay, these authentication measures will connect users to their actions. Rather than only knowing that someone faxed a patient file to a malpractice attorney, you'll know exactly who did.

• **Make images disappear.** As mentioned, devices store a picture of processed documents. Newer, better devices come with built-in tools to erase latent data from the hard drive. You can set your device to erase images automatically right after you use them or to do it manually on demand, such as when you are trading in the device.

• **Encrypt.** Certain documents, including frequently used forms and address books, may be deliberately stored on the device. Encrypt them so that unauthorized users can't see them today or when you retire the device.

• **Lock print jobs.** Require employees to swipe their smart cards or key in their PINs at the device to initiate printing. This eliminates the problem of printing jobs remotely and having them linger on the output tray.

• **Alert IT.** If the IT team is not already thinking about it, remind it about the need to secure these devices as if they were computers on the network. In reality, they are.

Most of these physical security steps come with the device as options. Third-party solutions let you take privacy and security a step further.

• **Get a fax server.** Faxes are still common in health care, and analog faxes are one of the least secure methods of transmitting information. Invest in a fax server to make faxing digital, and thus easier to secure—and save money in the process.

• **Filter your content.** New software lets users monitor communications to prevent certain content from leaving the in-house network—for example, content that includes Social Security numbers, credit card information, and diagnoses.

• **Secure your e-mail.** Generally, once you send an e-mail, it's out of your control. You can't determine who looks at it, if/where it's forwarded, and how it may change between recipients. Secure e-mail keeps the message in your own network

and requires "recipients" to log into your system and read the message there. In addition to corralling the content, it creates a rich audit trail of who looked at what when.

• **Audit trail software.** Robust audit trails go a long way toward pleasing auditors. While stock MFDs yield modest usage logs, enhanced software provides details about who did exactly what when. It simplifies catching misbehaving insiders and just may save your business in the event of litigation.

• **Password-protected scanning.** Even if you are requiring users of the scanner to authenticate their identities, you can further secure scanning. Require recipients to provide a password to read the scanned document you have sent them.

• **In other words, take control of your content.** Enterprise output, fax, and workflow management software can enable you to manage security and a host of other functions around your copiers, printers, scanners, fax machines, and MFDs, giving you control over the sensitive patient information entrusted to your care.

What Will This Cost?

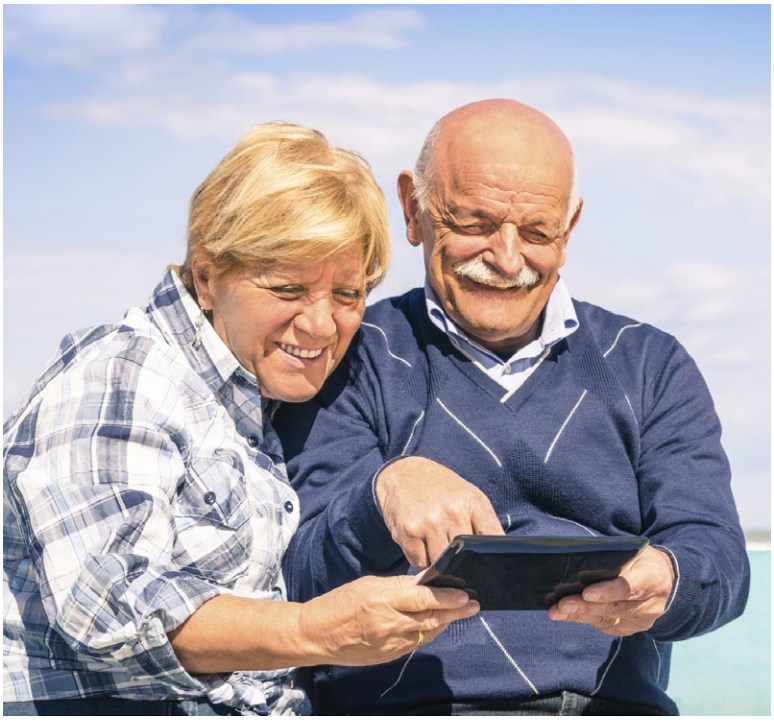
If you are a CFO, you are probably saying that these solutions sound great, and you certainly want to manage your privacy and security risks, but how much will it all cost?

Well, you do have to pay for it, but the good news is it often pays for itself in short order. For example, a cost-benefit analysis conducted by Ricoh Americas Corporation for a major hospital that was considering replacing its analog fax machines with a central fax server found that faxed documents were going to cost several cents per page, a cost the organization found to be prohibitive. However, when put into context and compared with the costs already being paid for analog faxing (which analysis revealed to be almost nine times as expensive), it was clear the cost savings were going to pay for the new gear in short order—and this is without putting a price tag on the security advantage.

Many of the technologies discussed here work the same way. Once you have figured out the savings and benefits in terms of efficiency and workflow, factor in the avoided costs of a potential security breach, litigation, auditing headaches, and reputation loss.

With a comprehensive approach to privacy and security, health care organizations can move from being simply in charge of their enterprise to being in control of it. It's a big difference and one that's worth the effort—before HHS comes calling, with your patients right behind them.

— Kash Hatton is manager of technical architecture for health care and Nannette Sloan is manager of process optimization for health care at Ricoh Americas Corporation.



Telehealth's Role in Reducing Readmissions

By Kathleen Flannery

A small but promising study yields evidence that telehealth can cut readmissions—and costs.

Hospital readmissions were a complex problem even before the federal government got involved. It can be challenging to devise the best strategy for helping fragile, often elderly patients continue to recover at home and avoid the return visits that are costly to their health as well as to the hospital. Adding to the urgency, hospitals now face penalties from the Centers for Medicare & Medicaid Services if their readmission rates are deemed excessive.

Could telehealth technology offer a solution? Kennedy Health System's experience with a remote patient monitoring program in its home care department yielded promising results: reduced hospitalizations and a net cost savings of $176,940.

Background

Kennedy Home Health Care is a division of Kennedy Health System in New Jersey, one of the states most penalized for high readmission rates. The New Jersey Hospital Association reports that a variety of strategies helped state hospitals reduce readmissions by 13% between 2010 and 2013. These include expanded follow-up care and greater use of telemedicine to track patients' vital signs and overall well-being, according to Kerry McKean Kelly, the association's vice president for communications and member services.

The Kennedy Home Health Care in suburban southern New Jersey handles an average patient population of 400. The hospital's goal for the 2013 telehealth study was to use remote monitoring to reduce the 30-day readmission rate for patients with chronic conditions.

The 29 postdischarge patients in the study had an average age of 77.4 and 90% were on Medicare. Slightly more than one-half (55%) were female. Their prior diagnoses were congestive heart failure (93%) and chronic obstructive pulmonary disease (7%).

Significantly, these patients had an average rate of 2.78 hospitalizations per year for disease exacerbations. A persistent problem in this population has been compliance with the details of their care. For some, it seemed that being in and out of the hospital had become a way of life.

Designing the Program

Kennedy Home Health Care arranged for remote monitoring for the 29 patients, using customizable equipment that allowed them to

provide detailed daily reports on their condition. A nurse visited each home to explain the program and equipment to the patients and, when appropriate, to family members.

Home care staff monitored patient responses daily via an Internet connection. If the responses or data raised concern—for example, sudden weight gain indicating fluid retention—the patient promptly learned of it. A nurse would phone patients as needed or pay them a visit to help them stay on track with their home care.

The emergence of telehealth has led to a proliferation of equipment options. In this instance, the choice was Authentidate's Electronic House Call system. Patients were supplied with an easy-to-use 8-inch color touchscreen. Considering this is not the tech-savvy population who are programming DVRs and posting photos on Twitter, the technology's simplicity was a crucial factor. The monitoring device included a built-in blood pressure monitor, a wireless weight scale, and a pulse oximeter.

At the other end, clinical staff used Authentidate's InscrybeMD, a telehealth Web application, for daily monitoring of patients' responses. Each patient's physician received a weekly report based on the data collected.

The price tag for the remote patient monitoring program was $4,200. Add a one-time hardware expenditure of $18,360, and the total cost came to $22,560.

Program and Results

Patients used the touchscreen to respond to daily questions. Again, these were designed to be user-friendly; they were framed at a sixth-grade reading level.

Questions for the heart failure patients included inquiries about their blood pressure, weight, pulse, medications, whether shoes or clothing felt tight, whether they were taking their diuretics, and how they had been sleeping. Chronic obstructive pulmonary disease patients had their own set of questions, with topics including use of nebulizers, trouble with coughing, and ease of breathing.

The problems encountered were minor—for example, temporary trouble getting a wireless signal—and generally remedied the next day.

Kennedy Home Health Care expressed satisfaction with the results. Patients had an average of 0.59 rehospitalizations during the one-year program, compared with the 2.78 hospitalizations previously. That number represented a reduction of almost 79%. Eight patients were readmitted to the hospital (cost: $76,000) while 21 were able to avoid readmission (cost savings: $199,500). Subtracting the program cost, there was a net savings of $176,940 and a 7.8 times return on investment.

This study did not survey patient satisfaction formally. However, patients expressed overall enthusiasm for the program. They said they felt much more attuned to their illnesses and symptoms, more responsible for their outcomes, and more involved in their care. This appears to be in line with the Utah Remote Monitoring Project (as reported by Laura Shane-McWhorter in June 2014), a similar program. That six-month study of 109 diabetes patients also using the Authentidate system reported a patient satisfaction level of 97.2%.

Physicians were supportive and played an important role in urging the patients to try the home monitoring system.

Overcoming Roadblocks

It is worth noting that while telehealth has been a success story in the VA health care system, lack of reimbursement has been a roadblock for other health care providers. In many states, including New Jersey, no reimbursement is currently available for telehealth services. Although small in scale, this study showed that telehealth can be successful in the private sector.

Reducing the amount of readmissions will involve hospitals doing more than sending patients home with a brochure. Innovations in remote monitoring are making systems more user friendly for patients as well as providers—with access via tablets and smartphones, for example. It is highly likely that the use of telehealth technology will grow as hospitals seek ways to safeguard the health of newly discharged patients, and reduce the high costs of readmissions.

— Kathleen Flannery is the administrator of Kennedy Home Health Care, a department of the Kennedy Health System in Voorhees, New Jersey. She has more than 30 years' experience in home care.