BY KIM RIBBINK

Piecing Together THE PRIVACY PUZZLE

As healthcare providers **PREPARE TO COMPLY** with the **PATIENT PRIVACY ISSUES** stemming from the **HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT**, the pharmaceutical industry will have to **FIND WAYS TO WORK** with business partners within the **CONFINES OF THE LAW** if they want to continue to gain access to data.

Starting in April 2003, patients will be granted unprecedented protection over the privacy of their medical records with the implementation of the Health Information Portability and Accountability Act.

The act guarantees patients access to their medical records, giving them more control over how their protected health information is used and disclosed and providing a clear avenue of recourse if their medical privacy is compromised, says the Department of Health and Human Services.

The act targets what is known as covered entities — health plans, healthcare providers, and healthcare clearinghouses — requiring that they

comply with rules to protect medical records and other protected health information, known as PHI.

HHS will seek to obtain voluntary compliance by organizations. However, the repercussions for covered entities that flout or fail to adhere to the law can be severe — with civil penalties of $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated. Criminal penalties are up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

On the surface, none of this directly applies to the pharmaceutical industry. But, a recent Datamonitor report — Facing HIPAA: What Pharmaceutical Companies Need To Know — points out that if pharma companies do not demonstrate at least an understanding of HIPAA regulations, they may find themselves cut off from information sources, which will impact upon all areas of their business.

A MAZE of Legalities

In 1996 Congress recognized the need for national patient privacy standards and, as part of HIPAA, set a three-year deadline for it to enact such protections. HIPAA also required that, if Congress did not meet this deadline, HHS was to adopt health information privacy protections via regulation based upon certain specific parameters included in HIPAA. Congress failed to enact health privacy legislation.

HHS proposed federal privacy standards in 1999 and, after reviewing and considering more than 52,000 public comments, published final standards in December 2000. In March 2001, HHS Secretary Tommy G. Thompson requested additional public input and received more than 11,000 comments, which helped to shape the improvements proposed in March 2002. The final improvements, issued August 9, 2002, reflect public comments received on that proposal.

Most covered entities have until April 14, 2003, to comply with the patient privacy rule, though certain small health plans have until April 14, 2004. The full impact of HIPAA on the industry is difficult to predict at this stage. But it will affect the gathering and distribution of data, particularly companies' dealings with key customers — the physicians.

"The impact of HIPAA on non-covered entities such as pharmaceutical companies will be through either business associate contracts, transaction standards, and the proposed security regulation chain of trust agreement," says Alexander J. Brittin, principal member of the Brittin Law Group PLLC.

Covered entities must comply with the Privacy Rule in their use of protected health information and disclosure to third parties — including pharmaceutical companies, explains Richard M. Campanelli, J.D., director of the Office for Civil Rights, Department of Health and Human Services. He says HIPAA does not prevent companies from gathering data for research purposes, but it does place strictures upon how that information may be disclosed by covered entities.

"The pharmaceutical company's approach to physicians has to take into account the fact that physicians are going to be much more restricted, by design and by regulation, as to the kind of information they share about their patient base," says Brian Jensen, senior consultant with Watson Wyatt Worldwide.

Key areas for companies to focus on are how does information flow into them, how is it used, and how does it flow out.

"Those three components are really what HIPAA is about," says Stephen W. Bernstein, co-chair of McDermott, Will & Emery's HIPAA Practice Group. "It's about what procedures and policies and expectations are built into the system and how these are managed. It's about consumer and customer relations."

While addressing the legal implications of HIPAA, companies also need to take into account state regulations as well as other federal statutes, such as 21 CFR Part 11, which establishes technical and procedural standards for electronic record keeping and electronic signatures.

"For most pharmaceutical companies this is a broader question and will vary greatly across the U.S.," says Sue Milam, Ph.D., director of client services at MyDocOnline Inc., a subsidiary of Aventis Pharmaceuticals. "The regulation depends on the role the company plays in the healthcare industry."

Research and Marketing IMPLICATIONS

Pharmaceutical companies rely on private and confidential patient data for research, marketing, and promotional initiatives, Datamonitor points out. HIPAA does not prevent companies from gathering data for research purposes, but it does place restrictions on how that information is gathered. There are a few ways companies can go about gaining access to PHI.

Covered entities must **COMPLY WITH THE PRIVACY RULE** in their use of protected health information and disclosure to third parties.

Richard Campanelli

For pharmaceutical companies, it can be as easy as putting training in place for their employees, adhering to certain standards that are HIPAA compatible, and **MAKING SURE THE PUBLIC KNOWS OF IT.**

John Mack

Healthcare providers, including pharmacies, which are directly covered by the HIPAA privacy rules, and their vendors, subcontractors, and agents may only **USE OR DISCLOSE THE MINIMUM AMOUNT OF PHI** that is necessary for that particular purpose.

Cheryl Camin

Key **AREAS FOR COMPANIES** to focus on are: how does information flow into them, how is it used, and how does it flow out. It's about consumer and customer relations.

Stephen W. Bernstein

"One way to get PHI data is that the covered entity can obtain specific authorization from individuals that their protected information can be disclosed," Mr. Campanelli says. "There also are exceptions where the covered entity can provide protected health information to third parties for public health or purposes under the Privacy Rule.

"For instance, for public-health purposes, the Privacy Rule permits a covered entity to disclose protected health information to an entity that is subject to FDA jurisdiction, if the disclosure relates to a FDA-related product or activity," he continues. "Many pharmaceutical companies may receive disclosures under this provision. Another common disclosure has to do with research. A covered entity can disclose protected health information to a pharmaceutical company if it has appropriate documentation of an IRB (institutional review board) or privacy board waiver of individual authorization for research."

According to Mr. Campanelli, generally these boards will issue a waiver if they determine that the research could not have practicably been done without access to the PHI; that the research could not have practicably been done without a waiver; and that it is not practical to get the individual's authorization for the research. In addition, the board needs to determine that disclosure of PHI involves no more than a minimal risk to the privacy of the individual.

The Privacy Rule also permits a covered entity to disclose what is known as limited data sets for research purposes. These limited data sets contain no directly identifying PHI. A "data-use agreement" must require the researcher to use the information only for research purposes and that the researcher promises not to disclose or attempt to re-identify the individuals from the information.

Some difficulties might arise in gaining public trust that the data a company is trying to gather will be used in a way that will not undermine PHI.

"It's very difficult to explain some of the ways in

The Relationship Between Covered Entities and Business Associates

THE HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT has a direct impact on how covered entities — healthcare providers, health plans, and healthcare clearinghouses — handle a patient's protected health information.

"HIPAA privacy rules provide restrictions on how an individual's protected health information may be used or disclosed," says Cheryl Camin, associate at the Dallas office of Gardere Wynne Sewell LLP. "Consequently, in many cases, healthcare providers, including pharmacies, which are directly covered by the HIPAA privacy rules, and their vendors, subcontractors, and agents may only use or disclose the minimum amount of PHI that is necessary for that particular purpose.

"In addition, often the individual is required to authorize a particular disclosure of his or her protected health information (PHI), for example in cases of using the information for marketing purposes," Ms. Camin says. "Also, covered entities and third parties that receive PHI must take precautions to safeguard the integrity of the PHI, and prevent impermissible uses or disclosures of such information."

Since pharmaceutical companies will continue to need access to PHI, particularly with regard to clinical trials, the impact of HIPAA in general will be impossible to ignore.

"Pharmacies are covered directly by the HIPAA privacy rules, however, a company manufacturing pharmaceutical products that receives PHI from a covered entity will be a business associate of that covered entity," Ms. Camin continues. "In this case, as a business associate, the pharmaceutical manufacturer will be required to safeguard the PHI and provide individuals with the rights to amend, restrict, have access to, and account for their PHI.

"In addition, the business associate must ensure that anyone else receiving the information from them adheres to the same requirements," she says. "All of these requirements, as well as other obligations are outlined in a business associate agreement that must be signed by both the covered entity and the business associate. Once the business associate signs the agreement, it is obligated legally to comply with many of the same privacy rule requirements as a covered entity, so either way they're covered by the privacy rule."

While there is some debate as to whether pharmaceutical companies fit the definition of business associates, since only in very unusual circumstances would they be conducting business on behalf of a covered entity, the fact remains that doing business with any healthcare provider covered by HIPAA will have a dramatic impact on the industry's access to, and use of, PHI.

which healthcare information is used in a fairly benign but very useful way," Dr. Milam says. "From a public-health perspective, for example, when population data is taken in the aggregate, it's very useful for treatment, patterns of illness behavior, etc. Under the rules, companies can use information in the aggregate, but they have to tell people that they're doing so and sometimes that sounds scary. So while it is good to increase awareness, perhaps this could create a little fear on the part of patients that there is something that they should be worried about."

IMPACT **on Marketing**

The biggest impact could be on some direct-to-consumer marketing activities, since HIPAA prohibits the use of PHI for strictly marketing purposes unless the covered entity has express, specific authorization from the individual.

"A covered entity could not disclose protected health information to a manufacturer to allow the manufacturer to evaluate the effectiveness of a marketing campaign for a prescription drug," says Cheryl Camin, associate at the Dallas office of Gardere Wynne Sewell LLP. "In this example, the disclosure is made for commercial marketing purposes and would require an authorization from the individual, as opposed to disclosures permitted for treatment, payment, or healthcare operation purposes."

In the case of pharmaceutical, biotech, and device companies, since most of them are not covered entities, but nevertheless live off data derived from covered entities, the key will be how they "reverse engineer" the process so that covered entities feel comfortable in providing data and know that this industry segment will sensitively handle the information in a manner consistent with HIPAA.

Because pharma's access to PHI will become a challenge under HIPAA, some barriers to current marketing practices will result, particularly in some areas associated with marketing.

"People who are accustomed to being able to market in very appropriate, but creative ways, will need to evaluate their practices to see how they actually fit or don't within the new rules when viewed from the covered entity's perspective," Mr. Bernstein says.

While this presents clear challenges for the industry, Mr. Campanelli adds that most of the industry respects the need to protect patient privacy and has restrictions in place.

Small STEPS **to Compliance**

Given the complexities and length of the regulations, companies will need to assess individual lines of business, the data that are currently used and how the data are obtained, and then develop ways to facilitate that continued flow in a way the data source/covered entity can live with under HIPAA and applicable state law.

It is important that a company performs these internal assessments, Datamonitor analysts say, to limit the necessary financial input and ensure that the compliance measures undertaken are coordinated with partnering pharmaceutical/biotechnology companies and covered entities.

"Organizations should do a department-by-department evaluation or assessment of the potential risks," says Herb Larsen, VP and product management at Quovadx Inc. "That means understanding where the data come from, identifying who has access to the data, establishing security mechanisms to keep someone from viewing data they shouldn't, and establishing policies and procedures to promote and provide guidance on compliant usage."

Mr. Bernstein suggests companies identify individuals within each line of business, including legal, sales and marketing, research/medical affairs, and others who require data from covered entities, begin to put themselves in the shoes of their data sources, and then build systems, processes, forms, and policies that will enable the data to continue to flow in light of HIPAA. HIPAA provides multiple pathways that allow data to flow — companies just have to identify the pathway that works best for their data source and them.

Also, experts recommend that companies appoint a privacy officer to manage the process.

"This person should be in charge of the review, and would look at all the processes that are in place — everything from phone interactions to documentation, medical records, and communications with other providers," Dr. Milam says.

The first step to ensuring across-the-board compliance is personnel training. A pharmaceutical company starting on the road to compliance needs to invest time, money, and people into achieving its goals, but without extra investment in the people, the time and money may well be wasted.

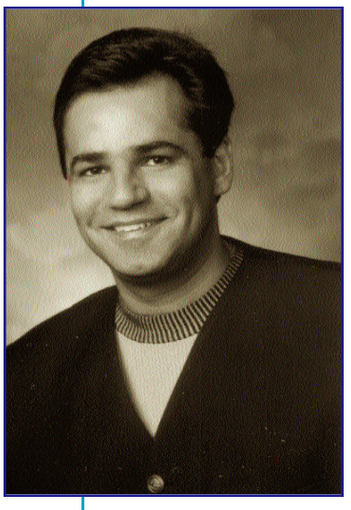
"Training is going to be a very important aspect for all organizations to make sure their workforce is skilled and knowledgeable in understanding two really critical aspects of the privacy rule," says Uday O. Ali Pabrai, CEO of the HIPAA Academy. "One is to ensure that all of the requirements are tied into the flow of PHI — inside and outside the organization. The second aspect is to learn, understand, and respect individual and patient rights."

The difficulty for companies is proving HIPAA compliance to consumers or business partners.

"I'm not aware of an existing certification that a company can achieve or receive that states it has 'the stamp of approval,' that it is now HIPAA compliant with privacy requirements and can go forth," Dr. Milam says. "When a group emerges that provides some kind of certification, it can be the badge that a company can refer to prove compliance. Until then, companies are really scared to say they are HIPAA compliant, because it's not clear yet what that means."

TECHNOLOGICAL **Solutions**

Perhaps the biggest aid to compliance will be technological solutions to information transfer.



TRAINING is going to be a very important aspect for all organizations to make sure their workforce is skilled and knowledgeable in understanding the privacy rule.

Uday O. Ali Pabrai

If companies cannot demonstrate compliance, they won't be in a position to assume any kind of market leadership because they will bump up against the **BRICK WALL OF CONFIDENTIALITY**.

Brian Jensen

Under the rules, companies can use information in the aggregate, but they have to tell people that they're doing so and sometimes **THAT SOUNDS SCARY**. So while it is good to increase awareness, perhaps this could create a little fear on the part of patients that there is something that they should be worried about.

Sue Milam, Ph.D.

Datamonitor analysts suggest that companies should either update or replace their software systems; ensure all data-management systems across the company are integrated; and ensure their software systems are outward-looking and able to interact with industry collaborators and covered entities.

"The big challenge for organizations is to find flexible and adaptable software and technology solutions that can help them to mitigate their risk and implement their best practices in line with their own business functions," Mr. Larsen says.

"As organizations start to better understand all the steps they need to take to become compliant, this will lead to substantial e-business-type activities and initiatives to protect that information," Mr. Pabrai says. "The legislation impacts the movement of electronic data between providers, the clearinghouses, as well as the payers. That's a huge component and a huge impact in terms of the industry building a framework to support electronic communication."

To adequately collect data, the pharma industry will need to give covered entities an assurance that its systems are secure.

"If data are sent to a company electronically, which more than likely will happen, that company will have to enter into a contract that states it will have the same level of security that the person sending the data does," Mr. Brittin says.

Many pharma companies have begun to address privacy issues in how they store and access data, and many more companies are offering technological solutions.

"We have installed into our product the same type of secure technology as financial institutions have; where the data are encrypted in a stand-alone system that is not available to the outside without a password and user ID," Dr. Milam says. "We have several layers of redundancy in our system to protect against the loss of information. We tried to anticipate the various issues that users were going to come up against in trying to adhere to these regulations."

MyDocOnline has faced questions from doctors as to whether using the product will make them HIPAA compliant. Legal advice has been that the company can't make that promise since what applies to a "covered entity" is different from what applies to a "business associate."

"What we can do on our end as a business associate is interpret the rules, evaluate, and become compliant," Dr. Milam says. "There are ways in which MyDocOnline can assist doctors in adhering to these rules they face — the protected communications, the documentation. But it is important that they seek advice about how HIPAA will affect a physician's office or a medical group."

What the Law Means and Who Will Enforce It

UNDER THE HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT, CONGRESS REQUIRED HEALTH PLANS, HEALTHCARE CLEARINGHOUSES, AND THOSE HEALTHCARE PROVIDERS WHO CONDUCT CERTAIN FINANCIAL AND ADMINISTRATIVE TRANSACTIONS ELECTRONICALLY (SUCH AS ELIGIBILITY, REFERRAL AUTHORIZATIONS, AND CLAIMS) TO COMPLY WITH EACH SET OF FINAL STANDARDS. OTHER BUSINESSES MAY VOLUNTARILY COMPLY WITH THE STANDARDS, BUT THE LAW DOES NOT REQUIRE THEM TO DO SO. AMONG KEY COMPONENTS OF THE LAW ARE:

- Patients must give specific authorization before entities covered by this regulation could use or disclose protected information in most non-routine circumstances — such as releasing information to an employer or for use in marketing activities. Doctors, health plans, and other covered entities would be required to follow the rule's standards for the use and disclosure of personal health information.
- Covered entities generally will need to provide patients with written notice of their privacy practices and patients' privacy rights. The notice will contain information that could be useful to patients choosing a health plan, doctor, or other provider. Patients would generally be asked to sign or otherwise acknowledge receipt of the privacy notice from direct treatment providers.
- Pharmacies, health plans, and other covered entities must first obtain an individual's specific authorization before sending them marketing materials. At the same time, the rule permits doctors and other covered entities to communicate freely with patients about treatment options and other health-related information, including disease-management programs.
- Specifically, improvements to the final rule strengthen the marketing language to make clear that covered entities cannot use business associate agreements to circumvent the rule's marketing prohibition. The improvement explicitly prohibits pharmacies or other covered entities from selling personal medical information to a business that wants to market its products or services under a business associate agreement.

OVERCOMING **Perceptions**

Datamonitor analysts say for reasons of public image, intelligence capabilities, research scope, and marketing it will become advantageous for pharmaceutical companies to demonstrate clear compliance with HIPAA law.

There has been a growing public perception that advances in electronic technology in the healthcare industry have led to a substantial erosion of privacy of healthcare information.

"I've always felt that the risk of an actual breach of confidentiality is more perception than a reality," Mr. Brittin says. "Most of these rules are based on a minority of the population's perception that their health information is being used improperly."

Dr. Milam adds that the federal government and many states passed legislation because of this perception of patients that their privacy was being violated.

Implementing HIPAA-compatible privacy and security standards may suggest to consumers and physicians that the pharmaceutical company is careful with all private information.

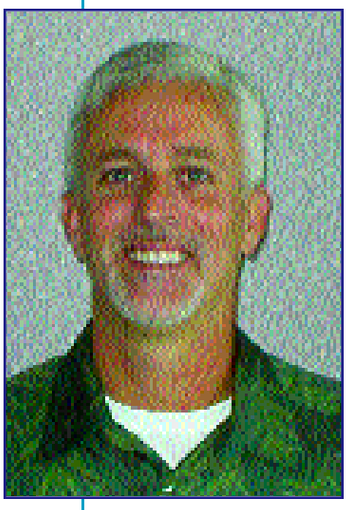
"A company can use HIPAA as a guideline for how it treats all types of personal information from consumers," says John Mack, president of VirSci Corp. "Pharmaceutical companies need to show that they are sensitive to the issues and are doing something about them. It can be as easy as putting training in place for their employees, adhering to certain standards that are HIPAA compatible, and making sure the public knows of it."

Sound BUSINESS **Practice**

Ensuring its databases and electronic transfers are safe, secure, and efficient will help the industry maintain the confidence of healthcare providers and potentially gain the trust of consumers. Furthermore, it has the added benefit of simplifying business processes.

"Compliance presents a huge opportunity for organizations, including healthcare providers, pharmaceutical industry participants, and the healthcare payer sector to really streamline their business processes by standardizing the administrative transactions, streamlining the flow, and eliminating a huge burden," Mr. Larsen says. "The pharmaceutical industry has the opportunity to begin to transact business in a standardized way, to eliminate the maintenance around the usage of proprietary systems and proprietary formats, and to get to more standardized repository-type information that could be farmed out for research purposes."

Creating greater efficiencies through e-business



Organizations should understand where the data come from, identify who has access to the data, **ESTABLISH SECURITY MECHANISMS** to keep someone from viewing data they shouldn't, and establish policies and procedures to promote and provide guidance on compliant usage.

Herb Larsen

● Patients generally will be able to access their personal medical records and request changes to correct any errors. In addition, patients generally could request an accounting of non-routine uses and disclosures of their health information.

HHS Secretary Tommy G. Thompson recently announced that the Centers for Medicare & Medicaid Services (CMS) will be responsible for enforcing the transaction and code set standards that are part of the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

"HIPAA administrative simplification is going to streamline and standardize the electronic filing and processing of health insurance claims, save money, and provide better service for providers, insurers, and patients," Mr. Thompson says. "To accomplish this will require an enforcement operation that will assure compliance and provide support for those who file and process healthcare claims and other transactions. CMS is the agency best able to do this."

CMS will continue to enforce the insurance portability requirements of HIPAA. The HHS Office for Civil Rights (OCR) will enforce the HIPAA privacy standards. CMS and OCR will work together on outreach and enforcement and on issues that touch on the responsibilities of both organizations — such as application of security standards or exception determinations.

Ruben J. King-Shaw Jr., CMS deputy administrator and chief operating officer, says CMS will create a new office to bring together its responsibilities under HIPAA, including enforcement.

The new CMS office will establish and operate enforcement processes and develop regulations related to the HIPAA standards for which CMS is responsible. These standards include transactions and code sets, security, and identifiers for providers, insurers, and employers for use in electronic transactions. The office will report directly to the deputy administrator.

The office also will conduct outreach activities to HIPAA covered entities, such as healthcare providers and insurers, to make sure they are aware of the requirements and to help them comply.

initiatives can help companies reduce costs, Mr. Pabrai notes.

"That's where HIPAA really provides a lot of opportunity for organizations," he says. "Companies will have to do it anyway. They may as well look at it strategically."

Mr. Mack says while there has been some confusion about whether or not pharma companies fit the definition of covered entities, the end result is the same. If pharma companies aren't prepared to work with covered entities under the new HIPAA regime, they'll find themselves cut off from data.

Many companies, including pharma, biotech, and medical-device organizations, already have undertaken steps toward HIPAA compliance.

"Because they service the healthcare industry, they need to know about HIPAA, examine it, and find ways to make the rules work for them and their data sources," Mr. Bernstein says. "Because these companies live off data, if they can't figure out a way to be user friendly in way that allows the covered entity to be compliant, they will quickly find that the data pipeline will be shut down."

Also, since it's the pharma company that knows best what data it needs and often has greater resources than most covered entities to devote to finding a "HIPAA-compliant" way to get the information, these companies often are in a better position to come to the table with an answer that can be helpful to the covered entity data source.

"If companies cannot demonstrate compliance, they won't be in a position to assume any kind of market leadership because they will bump up against the brick wall of confidentiality, one that has always been there," Mr. Jensen says. "But now this wall has big cement blocks of regulations standing behind it as well."

HHS remains confident that the end result of HIPAA compliance will be better business practices, and greater protection for consumers.

"What is envisioned and hoped for is that there will be a good cooperative relationship between physicians and other covered entities and the pharmaceutical organizations so that they will help each other comply with the Privacy Rule," Mr. Campanelli says. "Ultimately, our belief is that HIPAA will be good for the industry, good for the covered entities, and most important, it will be good for protecting the privacy of individuals' health information." ✦

PharmaVoice welcomes comments about this article. E-mail us at feedback@pharmavoice.com.

Experts on this topic

Stephen W. Bernstein. Co-chair, McDermott, Will & Emery's HIPAA Practice Group, Boston; McDermott, Will & Emery is an international law firm. For more information, visit mwe.com.

Alexander J. Brittin. Principal member, the Brittin Law Group PLLC, Washington, D.C.; Brittin Law Group specializes in healthcare and government contract counseling and litigation. For more information, visit brittinlaw.com.

Cheryl Camin. Associate, Gardere Wynne Sewell LLP, Dallas; Gardere Wynne Sewell provides legal advice, counsel, and strategic direction. For more information, visit gardere.com.

Richard M. Campanelli,J.D. Director, Office for Civil Rights, Department of Health and Human Services, Washington, D.C.; HHS, through OCR, promotes and ensures that people have equal access to and opportunity to participate in and receive services in all HHS programs without facing unlawful discrimination. For more information, visit hhs.gov/ocr/hipaa.

Brian Jensen. Senior consultant, Watson Wyatt Worldwide, Chicago; Watson Wyatt is a global consulting firm focused on human capital and financial management. For more information, visit watsonwyatt.com.

Herb Larsen. VP, product management, Quovadx Inc., Englewood, Colo.; Quovadx provides end-to-end total business infrastructure and integration solutions. For more information, visit quovadx.com.

John Mack. President, VirSci Corp., Newtown, Pa.; VirSci provides pharmaceutical and other healthcare clients with privacy, HIPAA, and e-health best practice intelligence. For more information, visit virsci.com.

Sue Milam, Ph.D. Director, client services, MyDocOnline Inc., Round Rock, Texas.; MyDocOnline, a subsidiary of Aventis Pharmaceuticals, provides customized Internet applications that enable physician practices to improve overall efficiency while enhancing patient-physician interaction. For more information, visit mydoconline.com.

Uday O. Ali Pabrai. CEO, the HIPAA Academy, Clive, Iowa; HIPAA Academy delivers solutions to assist organizations with their HIPAA initiatives. For more information, visit hipaaacademy.net.