Oncology Issues

ISSN: 1046-3356 (Print) 2573-1777 (Online) Journal homepage: https://www.tandfonline.com/loi/uacc20

HIPAA: Changing the Health Care Landscape

Kent Giles

To cite this article: Kent Giles (2000) HIPAA: Changing the Health Care Landscape, Oncology Issues, 15:4, 21-23, DOI: 10.1080/10463356.2000.11905144

To link to this article: https://doi.org/10.1080/10463356.2000.11905144

Published online: 17 Oct 2017.

HIPAA: Changing the Health Care Landscape

by Kent Giles, M.P.P.M.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), signed into law on August 21, 1996, is clearly the most significant health care legislation since the creation of Medicare. Its far-reaching impact will affect hospitals, payers, and physician practices in nearly every area of operations.

HIPAA contains five sections, or "Titles," of requirements and standards, which apply to virtually every provider, payer, and clearinghouse in the United States. Title I covers health access, portability, and renewability. Title II focuses on preventing health care fraud and abuse. Title III pertains to tax-related provisions and medical savings accounts. Title IV addresses the application and enforcement of group health plan requirements. Title V focuses on revenue offsets.

Unlike many federal health initiatives that have been enforceable only for Medicare or Medicaid providers, HIPAA governs all health care providers, payers, and clearinghouses that choose to transmit or maintain individually identifiable patient information in electronic form. This patient-specific information is known under HIPAA as protected health information. HIPAA's definition of electronic format includes computer diskette, storage on a computer server, e-mail, magnetic computer tape, voice recordings, and similar media. HIPAA also governs the progeny of protected health information, such as printouts or reports. Since virtually all health care entities use electronic media to store and/or transmit claims, virtually all must be compliant with the administrative simplification provisions of HIPAA within two years of the final release dates for each set of regulations. Only small health plans with less than 50 members are exempt from this; they have a three-year compliance window.

Kent Giles, M.P.P.M., is senior manager, Health Care Information Risk Management, at KPMG, Atlanta, Ga.

ASSESSING THE IMPACT OF HIPAA

The impact of Title I on improving health access, portability, and renewability of coverage has been widely debated. Some estimate that Title I provisions, which were projected to benefit tens of millions of Americans, have benefited less than 500,000 people. Other estimates hold the impact at more than 3 million beneficiaries.

Estimates of benefit are difficult to find on the impact of Title III (tax-related provisions), Title IV (application and enforcement of group health plan requirements), and Title V (revenue offsets).

Of all the components of HIPAA, the fraud and abuse provisions in Title II combined with greatly increased federal funding for the Office of Inspector General (OIG) will likely have the greatest impact on providers and payers. Increased conviction rates, penalties, and court actions will help to recover some of the estimated 11 cents on every health care dollar that the Work Group for Electronic Data Interchange (WEDI) estimates is attributable to fraud and abuse. Increasing the chance of being "caught" will likely help deter intentional fraud and abuse while increasing the resources expended on preventing improper coding.

Standardized transactions and identifiers will also help to reduce common billing errors and provider costs through greater levels of automation. For example, standardized certifications that are available online as opposed to "on hold" will help reduce administrative costs.

On the downside, one of the most alarming of HIPAA risks for hospitals is the potential to lose accreditation by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) for overall HIPAA non-compliance. Various other accrediting organizations governing research grants and other entities such as the American College of Surgeons may also require HIPAA compliance.

In the end, non-compliance with HIPAA would eventually render the hospital or provider unable to conduct business or render care because it would no longer be able to receive reimbursement or conduct transactions with payers, other providers, the government, or any other HIPAA-defined business partner.

UNIFORM NATIONAL TRANSACTION STANDARDS

One of the most positive aspects of HIPAA is the creation of uniform national transaction standards for all health plans, employers, providers, payers, and clearinghouses. Rather than allowing individual states and/or payers to continue requiring conflicting standards for transactions, code sets and identifiers, HIPAA is standardizing formats nationally in an effort to encourage widespread use of electronic data interchange

(EDI). Because EDI can significantly reduce the costs associated with manual transactions such as phone inquiries, this level of uniformity has long been requested by the health care industry.

Imagine an environment in which having a business office employee call and wait on hold for a half an hour to obtain a pre-certification number or verify coverage is replaced by an online computer-based transaction. Further, imagine the day when copying surgical notes, radiology and lab reports, and faxing these records to a payer is handled electronically.

WEDI estimates that EDI has the potential to save providers $9 billion and the overall system (including the federal and state governments, payers and employers) $26 billion per year. Other studies show as much as $1.30 per claim saved by submitting claims electronically versus paper. For small providers that cannot manage EDI transactions, HIPAA allows them to use a clearinghouse that is HIPAA compliant. As an added incentive to use electronic claims submission, HCFA will begin charging $1 surcharge per paper claim filed for Medicare reimbursement.

Many skeptics of HIPAA cite the numerous failings of prior federal initiatives to save providers money and regard HIPAA's security and privacy provisions as "unfunded federal mandates." They are correct. Others are guardedly optimistic and cite the numerous advantages of EDI and industrywide standardization. They also are correct, if EDI is implemented uniformly. In the end, the truth is that HIPAA creates a balancing act between additional costs for security and privacy (an unfunded federal mandate) and savings or revenue enhancements attributable to reduced administrative costs and improved cash flow via faster claims payment.

STANDARDIZATION AND CORE SECURITY REQUIREMENTS

WEDI estimates that 26 cents out of every dollar spent on health care is consumed in the reimbursement process, which varies considerably among organizations across the nation. There exist a myriad of differing transaction procedures, including authorizations, claims submissions, provider payments, and coordination of benefits transactions.

> The regulations are expected to be released August 2000 but do not go into effect until two years after the rule is published.

Title II attempts to remedy this situation by mandating and rewarding standardized transaction formats for enrollment/disenrollment, premium payments, remittances, eligibility, claim remittance, claim encounter, COB, claim status, claim attachments, referrals, certifications, authorizations, and first report of injury. It also rewards single national identifiers for patients, providers, employers, and payers. Finally, Title II encourages uniform national code sets by mandating the use of ICD-9-CM codes (ICD-10-CM, when available) for diagnosis. For procedures, it requires the use of ICD-9-CM, volume 3, or CPT-4 codes, as well as ICD-10-PCS or CPT-5 (includes HCPCS), when available.

HIPAA mandates following many administrative procedures designed to protect privacy, including certification of compliance, chain-of-trust partner agreements, contingency plans, formal mechanisms for processing records, information access controls, internal audit standards, personnel security, security configuration management, security incident procedures, security management processes, security training, and termination procedures.

Providers must maintain chain-of-trust agreements with all parties with whom they share individually identifiable patient information. These chain-of-trust agreements must include language that requires each data partner to certify to the other and to each organization in the chain of trust that they are HIPAA compliant. Third-party reviewers are the most cost effective and practical way to fulfill this requirement, because the alternative would be for each organization to be required to either certify itself and/or audit every business partner in its chain of trust.

Partners in the chain of trust include all payers, providers, employers, clinical service vendors (such as labs and radiology), and others with whom the institution shares patient-specific information.

In addition to these administrative requirements, HIPAA details numerous technical security mecha-

The Downside of Proposed Privacy Regulations

The proposed privacy regulations issued by the Department of Health and Human Services in November 1999 "may never go into effect," said Alan K. Parver, J.D., "because Congress could intervene and enact a new privacy statute before the regulations are finalized." Parver, a partner with Powell, Goldstein, Frazier, and Murphy LLC in the firm's Washington health care group, was a featured speaker at ACCC's 26th Annual National Meeting, held March 15-18, 2000 in Washington, D.C. The controversial regulations have generated 55,000 comments. The regulations are expected to be released August 2000 but do not go into effect until two years after the rule is published.

Controversy has arisen over several provisions. For instance, covered entities may not use or disclose health information unless authorized by the patient or for purposes of treatment, payment, or operations (minimum necessary disclosure). Also, the covered entity does not have to get authorization from the patient to disclose information for national priority activities (such as oversight of the health care system, including quality assurance activities, research, law enforcement, among others).

According to Parver, patients may request limits on use for treatment, operations, or payment; may withhold consent for other purposes (such as research); must receive written notice of privacy practices; and can access records and make corrections, which would be a new national right if the regulations are finalized.

Required internal administrative structures would be costly. The cost of implementing these regulations is estimated by Blue Cross/Blue Shield to be $40 billion, while HHS estimates are $3.8 billion, Parver said. If the $40 billion price tag is correct, then a 4 percent additional cost is projected on the health care system among other consequences, he added. Institutions would also have to designate a privacy officer.

Another problem with the proposed regulations, said Parver, is that "there never was established a baseline on the current state of patient protection" to determine the effect the proposed regulations would have. This raises uncertainty and concern.

Parver believes that as the debate continues the tendency will be to lean to a national standard over state rules. Having a patchwork of state rules makes compliance difficult for multistate entities and would continue the current uncertainty surrounding privacy issues. In the coming years, congressional interest in the privacy debate is expected to increase significantly.

nisms designed to protect data, including audit controls, authorization control, data authentication, communications and network controls, audit trails, encryption, entity authentication, event reporting, integrity controls, message authentication, message integrity, and user authentication. Failure to comply can result in substantial costs as well as in criminal and civil penalties.

SUMMARY

HIPAA need not be feared if it is effectively managed and becomes a top management priority. Experience has shown that time and money are inversely related. Therefore, organizations that begin HIPAA awareness, assessment, and planning now will be in the best position to manage HIPAA costs. Unfortunately less than 25 percent of hospitals and less than 5 percent of physician practices have initiated HIPAA compliance activities. Many cite the huge expenditures on Y2K as having left them without adequate resources to prepare for HIPAA. Unfortunately for them, HIPAA compliance is mission critical and resources must be dedicated or organizational mission may be jeopardized.

All providers are required to meet HIPAA standards within two years (sometime in 2002) of the release of each final standard. Successful implementation depends on leadership and budgetary support from top management, as well as a dedicated project team. This team should be comprised of individuals that are knowledgeable in clinical processes and understand health information security and privacy. The team should include experts in the organization's business processes, e-commerce, organizational policies and procedures, compliance issues, HIPAA, process redesign, and change management.

Unlike Y2K, HIPAA is not a one-time event. It is the law and a permanent component of health care strategy and tactics. Thus, success in preparing for HIPAA demands an ongoing program of assessment, planning, and implementation. Finally, compliance with security and privacy standards will initially increase costs. However, greater utilization of EDI can reduce costs and enhance revenues in the long term if processes and systems are improved.

The risks and rewards associated with HIPAA are numerous. The time to begin preparation is now.