

10 HIPAA tips for the physician office

Save to myBoK

by Steven S. Lazarus, PhD, FHIMSS

The Health Insurance Portability and Accountability Act (HIPAA) and its accompanying regulations present opportunities and concerns for physician practices. Many of the HIPAA requirements and issues are the same for physician practices as they are hospitals and other providers. However, small to mid-size physician practices have the flexibility to choose security strategies appropriate to their size and available resources. Here are 10 tips for physician offices to prepare for HIPAA.

1. Identify opportunities, benefits, and costs. The "[Quick and Dirty HIPAA Benefit Calculation Estimator](#)," below, can help offices quickly identify areas of potential benefit and estimate the potential financial impact for the transactions and identifier standards.

Consider this example: in one case, 20 medical groups, most of them with eight or more physicians, estimated an average annual potential benefit of \$7,200 per provider, exclusive of implementation and annual operating costs. Potential business operation savings were identified in the following areas:

- business office-51 percent
- managed care-12 percent
- bad debt, postage, etc.-37 percent

These benefits are obtainable by implementing the transaction standards. They involve increasing the utilization of electronic claims submission to most health plans and implementation of electronic remittance advice, eligibility inquiry at the time of registration/appointment scheduling, electronic referral authorization processing, and claims status inquiry.

Also, consider the cost of implementation and ongoing operation. There may be significant consulting fees, practice management system enhancement charges, and an increase in clearinghouse fees associated with implementing these changes. The range of cost will vary among organizations.

A significant contributing factor is the current practice management system’s capability to support the work flow and transaction data set requirements for the practice. In some cases, existing maintenance agreements will cover the cost of necessary enhancements; in others, additional fees for upgrades will be required, or total system replacement will be needed to achieve these capabilities.

quick and dirty HIPAA benefit calculation estimator

Organization Name:

	(1) Number of Staff	(2) 50% of (1)	(3) Salaries, benefits & overhead for (2) per year
1. Business Office - Staff posting paper insurance remittance			\$

- Patient and insurance collections staff - Error correction and insurance rebilling staff			
2. Managed Care Coordination - Precertification/preauthorization staff - Eligibility and benefit verification			\$
3. Cash to bottom line - Patient bad debt in dollars x 25% - Insurance denials for lack of preapproval or timely filing - 50% of postage and fees for patient statements	N/A	N/A	\$
Total annual operation saving potential (excluding EDI setup and transaction fees)	N/A	N/A	\$
Savings per provider FTE: total savings divided by FTE	N/A	N/A	\$

© Boundary Information Group 2000 (Assumes implementation of all standard transactions, code sets, and identifiers)

2. Be prepared for new provider IDs. The proposed rule for a standard provider identifier called for industry comment on a new way of standardizing provider identifiers. Once the final rule is published, we will know the specification of the identifier and the process for assignment to providers. When the final rule is published, be prepared to understand your responsibilities to apply for, receive, and use these new identifiers.

3. Use HIPAA resources developed by industry experts. There are many resources at your disposal. AHIMA has developed HIPAA training resources, including an Internet-based education program to learn about HIPAA at low cost from the practice setting (go to www.ahima.org). The Medical Group Management Association (MGMA) has produced national audio conferences on HIPAA, which are also available on audio tape (go to www.mgma.com). The Workgroup for Electronic Data

Interchange (WEDI) has developed a tool for implementing security called the HIPAA Security Summit Guide (go to www.wedi.org).

WEDI has also initiated a Strategic National Implementation Process (SNIP) to help the healthcare industry implement HIPAA. Industry experts are developing recommendations for HIPAA implementation in the additional form of educational programs, white papers, quarterly consensus building meetings, and workgroup discussion and consensus building through listservs addressing education, security and privacy, and transactions and code sets (go to www.wedi.org/snip).

4. Check out security tools. Several free and low-cost tools can assist organizations in structuring their security analysis. These include the HIPAA Security Summit Guide and the WEDI SNIP Security White Papers, which are available at www.wedi.org.

The North Carolina Healthcare Information and Communications Alliance Inc. (NCHICA) has developed a HIPAA security business impact analysis or gap analysis access database tool called EarlyView. The tool structures an assessment and documentation process consistent with the compliance requirements of the proposed security rule. Information about EarlyView can be obtained at www.nchica.org.

5. Use the Internet. Expert advice and opportunities for sharing information and concerns about HIPAA implementation abound on the Internet. Relevant Web sites and listservs include:

- American Health Information Management Association (AHIMA), www.ahima.org
- American Health Lawyers Association, www.healthlawyers.org
- HIPAAlive listserv, www.hipaadvisory.com/live
- Medical Group Management Association (MGMA), www.mgma.com
- US Department of Health and Human Services (HHS), <http://aspe.os.dhhs.gov/admsimp>
- Workgroup for Electronic Data Interchange (WEDI), www.wedi.org
- Boundary Information Group HIPAA resources, www.hipaainfo.net, see articles

If you do not have access to the Internet, it would be a good idea to obtain access for the purposes of HIPAA education and resources. The Internet is one of the primary media being used to disseminate information about HIPAA implementation. The cost of accessing the Internet for a year is less than the cost of the travel and registration fee associated with a two- to three-day HIPAA education program.

6. Understand your vendor's plan. Items that should be considered in assessing a vendor's preparation and HIPAA impact include:

- ability to handle the current and new provider identifiers during the transition
- ability to handle current and new standard code sets to support the transactions
- ability to produce outbound standard transactions that you want to implement (e.g., claims submission, eligibility inquiry, referral authorization request)
- ability to support inbound electronic transactions that you want to implement (e.g., electronic remittance advice, eligibility verification, referral authorization approval/denial)
- ability to support eligibility verification at the point of registration/appointment scheduling
- ability to store and retrieve authorization approval
- need to modify existing contractual agreements to include chain of trust, adherence to specify security and privacy policies and practices, and the acceptance of reasonable penalties to failure to support your HIPAA compliance requirements
- need to review vendor licensing requirements if the practice changes from shared user IDs to individual user IDs and the result has an impact on a number of licenses required

7. Prepare for internal education and training. Prepare an internal education program to acquaint all physicians and staff with HIPAA and its requirements. To the extent available, use educational information developed by national trade and professional associations and industry workgroups.

8. Put documentation in place. Compliance with security and privacy requires documentation. The business impact analysis, decisions that the practice makes to correct identified deficiencies, verification that the deficiencies have been corrected, and ongoing monitoring and auditing all must be supported by documentation. Make this an ongoing part of the process.

9. Monitor and review. The proposed security rule requires an ongoing monitoring and review process. Any organization that is a covered entity (such as a provider) needs to continue to monitor the performance of a security program and remedy significant issues.

10. Plan for change. HIPAA is an ongoing process. In addition to the final and draft regulations, HHS is working on additional regulations addressing enforcement, electronic claims attachments, and a standard health plan identifier.

Standardization of identifiers, code sets, data transaction formats, and security and privacy issues are motivated by administrative simplification and the potential for cost savings. Investments will be required to achieve this standardization, and those who fail to comply will face penalties. The key strategic decision for physician practices and all covered entities at this time is to decide whether HIPAA will be addressed as a compliance program only-or if the organization will also attempt to identify and take advantage of the potential benefits.

Steven Lazarus is president of The Boundary Information Group, a strategic alliance of consulting firms that offer complementary services in the management of healthcare information, in Denver, CO. He can be reached at sslazarus@aol.com

Article citation:

Lazarus, Steven. "10 HIPAA Tips For the Physician Office." *Journal of AHIMA* 72, no.2 (2001): 55-57.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.