

HIPAA Transactions and Code Sets Phase Plan to becoming Compliant

Model Compliance Plan for Extension and Project Plan

The Centers for Medicare & Medicaid Services (CMS) issued a model compliance plan that will allow health plans, health care clearinghouses and health care providers to receive a one-year extension to comply with the HIPAA rule governing electronic health care transactions.

The original deadline for compliance with the electronic transactions rule is Oct. 16, 2002 for all covered entities except small health plans, which by law had an additional year. Last year, in the Administrative Simplification Compliance Act, Congress authorized a one-year extension – to Oct. 16, 2003 – for those covered entities required to comply in 2002. To obtain the extension, a covered entity must submit a compliance plan on or before Oct. 15, 2002. Covered entities can use the model plan for this purpose.

A covered entity will be able to submit its extension plan electronically through the CMS Web site and CMS will provide an electronic confirmation of receipt of the plan. Covered entities also have the option of submitting their own version of an extension plan that provides equivalent information and can submit a plan on paper. Instructions for filing a plan are available on the Web site.

Under the Administrative Simplification Compliance Act, health care plans and providers must submit information on their compliance activities, including budget, assessment of compliance concerns, whether a contractor or vendor might be used to help achieve compliance, and a schedule for testing to begin no later than April 16, 2003.

The model compliance plan, and instructions on how to complete it, is available at www.cms.hhs.gov/hipaa/hipaa2/ascaform.asp. Electronic submission capability is available on the Web site. The model compliance plan and instructions were published in the April 15, 2002 Federal Register.

PHASE 1: Project Initiation and Assessment

Activities

1. Establish Executive Level Steering Committee to provide:
 - a. Organizational Leadership
 - b. Evaluation of Compliance Direction and Requirements relative to the organization.
 - c. Provide HIPAA Compliance Project Oversight and Funding
2. Establish HIPAA Project Office or Project Team (as necessary) to:
 - a. Education and awareness training for executives and staff on HIPAA Requirements and the current status of new and additional pending legislation
 - b. Conduct Initial Internal Resource Interviews.
3. Introduce Project
 - a. Determine Scope and Complexity
 - b. Identify Workgroup Leadership and Participants from Line of Business
 - c. Validate Tools and Templates
 - d. Mobilize and train Functional Workgroups comprised of Line of Business Reps to perform initial baseline gap analysis for EDI, Code Set, Security, Privacy and any other new or additional HIPAA requirements in their assigned areas of expertise including (but not limited to):
 - i. Medical Records
 - ii. Patient Accounting
 - iii. Clinical / Departmental
 - iv. Corporate Administration
 - v. Information Systems
 - vi. Other Areas
 - e. Perform Communications Network Security Architecture Review, Assessment and Network Penetration Testing
 - f. Executive Decision on HIPAA EDI Transaction Methodology
4. Determine System Changes and Continued Reliance Upon Clearinghouse to Transmit EDI and Code Set Compliant Transactions (minimal cost)-Continue to pay Transaction Fees
 - a. Use combination of Hospital System Changes and Clearinghouse to Achieve Partial/Basic Compliance-Continue to pay Transaction Fees
 - b. Make required changes to all business and ancillary/departmental systems in order to achieve full HIPAA compliance (as understood at that time)
5. Based upon Items One and Two, Document and Present HIPAA Compliance Action Plan and Multi-year Implementation Timeline to Executive Level Steering Committee for review, approval and funding as needed

PHASE 2: Implementation of HIPAA Compliance Action Plan

Activities:

1. Selection and training on appropriate HIPAA toolsets and methodologies
2. Selection, Training and Implementation of formal Problem and Change Management tools, policies, procedures and meetings to be implemented for the duration of the HIPAA project-if not in place today
 - a. This step provides timely problem identification, notification, tracking and escalation of unresolved problems that may be caused by required changes to the hospital's systems, the hospital network, vendor or e-commerce partner systems
3. Recommend and Adopt policy of Minimal System and Application Changes during the HIPAA Compliance work so that:
 - a. Internal Resources are primarily focused on HIPAA and performing other system and application changes is done on "emergency needs" basis, resulting in HIPAA work getting done quickly and for minimal cost
 - b. Minimal disruptions are caused to end user community due to number and severity of changes
4. Facilitate routine Workgroup or Project Team Status Meetings with minutes and updated Project Plans.
5. Implement routine Status Report to Executive Level Steering Committee
6. Legal Council Review of all vendor, partnership and physician practice agreements that provide access to either the hospital network and/or patient data. Update, replace or negotiate new policies to enforce HIPAA required EDI Transaction compliance, Privacy, Security, recoverability in event of accident or disaster and other HIPAA defined requirements as needed and as they become law.
7. Legal Council Review of New HIPAA Privacy and Security Policies and Procedures
 - a. Additional Review and Approval as may be required by state and local authorities
8. Approval of new HIPAA Privacy Officer and possible compliance manager(s) positions as needed by location and size of enterprise
9. Creation, Publication and Distribution of new HIPAA Privacy and Security Policies and Procedures Manual(s), including Privacy and Security Checklists for ongoing compliance use by HIPAA Compliance Officers or use by management
 - a. Appropriate Departmental or Functional Area Training and Certification on new HIPAA Policies and procedures so that existing employees can receive training and ask questions
 - b. Creation of HIPAA training and certification programs for new and temporary employees
 - c. Creation of internal employee and external patient complaint/abuse mechanisms as part of ongoing compliance efforts
10. Create training mechanisms, policies and procedures for HIPAA Compliance Officer as well as other desired positions, such as Privacy Compliance Manager or Security Compliance Manager
11. Creation of HIPAA Security and Privacy Compliance Reports for Management
 - a. Include creation, publication/distribution and Executive Review and Sign-off. Executive-Sign off is recommended due to the severity of HIPAA related fines and jail-time
 - b. Create HIPAA Report archival system and/or facilities for future inspection of reports by outside inspection entities (To be determined)
12. Modify the above procedures to incorporate additional HIPAA requirements such as Electronic Signature or National Individual Identifier as they become closer to reality and/or become law

PHASE 3: Testing and Implementation of HIPAA Compliant Systems, Applications and Technology

Activities:

1. Design HIPAA compliance tests and review HIPAA testing schedules for all internal systems and applications with HIPAA mandated changes. Add volume tests and perform capacity planning for response time sensitive applications and potentially elongated batch cycle work.
2. Demonstrate and document successful testing of all individual internal systems that have had HIPAA modifications made to them. Report on results of capacity planning measurements and recommend necessary hardware and software upgrades to provide reasonable response time and/or batch cycle processing time
3. Information Systems and HIPAA Test Managers perform Step 1 using any new network hardware and/or network monitoring and security packages. Monitor the network performance for potential bottlenecks or performance restrictions including hub and router ports with very high use, segments with high utilization, etc.
4. Recommend network component upgrades as necessary to guarantee performance, recovery/redundancy and security as required
5. HIPAA Test Managers design and review system wide test schedules and procedures for HIPAA Compliance once all individual systems have been tested
6. Schedule Testing for all HIPAA required transactions
7. HIPAA Test Managers design and review system wide test schedules and procedures for Internal HIPAA Compliance Certification Testing with outside agencies, payors and insurance companies
8. Document successful testing by EDI transaction type and number with outside agencies, payors and insurance companies. Include screen prints, printouts, and documented test plans as part of overall Internal HIPAA Compliance Certification Testing. Include proper management or executive signoff and appropriate emails to document as well. Compliance Officer should retain all copies for future reference and proof of successful testing in addition to the transaction testing
9. Check and update all system documentation and recovery procedures to reflect the new HIPAA compliant environment, including all EDI Transactions, EDI Transaction System Recovery Procedures, new encrypted backup and recovery procedures performed onsite or offsite, new network security, security password and intruder detection and network monitoring procedures, authorized application access, use of tokens or certificate authorization and authorization servers
10. Create education and training plans for end-users of new EDI transactions, Code Sets, Identifiers, and new Privacy and Security system or application modifications as made for HIPAA Compliance to nursing and clinical systems that require retraining or additional training for use, such as new features, biometric devices, etc.