HIPAA & the States: Critical Issues and Compliance Strategies

Summary
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) will require the most expansive and costly review of state government operations since preparing for the year 2000 computing crisis (Y2K). It has even been suggested that HIPAA compliance will cost states more than the $3.5 billion they incurred during Y2K.¹

Under HIPAA, administrative simplification is the common name given to seven different federal regulations that collectively require covered entities to:

- ensure individually identifiable health care information remains confidential and secure (i.e., privacy and security rules); and
- standardize how administrative and financial health care information is exchanged electronically (i.e., electronic transactions rules).

For states, achieving HIPAA compliance will require a labor-intensive review of how protected health information flows throughout state government. Even agencies exempt or not mentioned in statute will have to assess their reliance on individually identifiable health information from covered entities and comply with HIPAA standards.

For states, the large scope of HIPAA will mean that compliance costs could exceed those incurred during Y2K. Yet many state agencies continue to mistakenly believe they will not be affected by HIPAA. According to one survey, 57 percent of state and local government agencies did not know whether a central HIPAA project management office had been established in their state or whether an individual had been appointed to oversee HIPAA compliance activities statewide.²

Identifying which state agencies and programs will be affected by HIPAA will require a comprehensive assessment of how health information is collected, stored, used, and shared throughout state government. Once identified, the critical challenge will be for affected agencies to work collaboratively in achieving compliance to ensure programs continue functioning with minimal disruption.
Finding the resources to comply will be difficult. Though limited, only state Medicaid programs will receive federal matching funds to offset their compliance costs. However, states can better manage HIPAA’s impact by:

- coordinating compliance activities among the affected agencies;
- collaborating with the private sector; and
- developing and sharing innovative compliance tools.

What is Administrative Simplification?
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) will require policymakers to fund and manage the most comprehensive review of state systems since the year 2000 computing crisis (Y2K). However, the law’s complexity—combined with a staggered implementation and vague federal guidance—has made it difficult for states to determine the level of effort needed to achieve compliance.

Under HIPAA, administrative simplification is the common name given to seven different federal regulations issued by the U.S. Department of Health and Human Services (HHS). Collectively these rules require states to ensure individually identifiable health care information remains confidential and secure (i.e., privacy and security rules). They also require states to standardize the way administrative and financial health care information is exchanged electronically (i.e., transactions and codes, and identifier rules). These rules are summarized in Appendix A.

Achieving compliance with the administrative simplification rules has been a topic of much debate at the local, state, and national levels. The rules are extremely technical and use many terms unfamiliar to those not involved in the day-to-day administration of health care. Compounding this problem, HHS has made final only two of the seven administrative simplification rules it expects to release: (a) privacy and (b) electronic transactions and codes. These rules have left many questions about how state agencies and programs will be affected.

Because there is no precedent on which to base a response, preliminary compliance cost estimates have varied widely among states. In California, the state Medicaid agency estimated its costs would be more that $100 million over several years. Pennsylvania estimated statewide compliance costs (Medicaid and non-Medicaid combined) could fall between $50 million and $200 million. A similar impact assessment in Indiana suggested statewide compliance costs outside of Medicaid could reach $160 million.

It has been suggested that achieving HIPAA compliance will cost states more than the $3.5 billion they incurred during Y2K. State Medicaid agencies will receive limited matching funds from HHS to help offset their compliance costs. However, HHS has acknowledged it does not have enough information to estimate the fiscal impact for states outside of the Medicaid program and that even its current cost estimates for state Medicaid agencies may be underestimated.

Identifying which state agencies and programs will be affected by HIPAA will require a comprehensive assessment of how health information is collected, stored, used, and shared throughout all of state government. Once identified, the critical challenge will be for these agencies to work collaboratively in achieving compliance to ensure programs continue functioning with minimal disruption.
Identifying Covered Entities

The most immediate compliance challenge states face is determining which agencies and programs will be affected by HIPAA. HIPAA leaves individual states to decide which of their agencies and programs meet the definition(s) of a covered entity and are therefore subject to compliance. The law defines covered entities broadly as:

- **Health plans**, which are individual or group plans (or programs) that provide health benefits directly, through insurance, or otherwise.

- **Health care providers**, which are providers (or suppliers) of medical or other health services or any other person furnishing health care services or supplies, and who also conduct certain health-related administrative or financial transactions electronically; and

- **Health information clearinghouses**, which are any public or private entities that process or facilitate processing nonstandard health information into standard data elements.5

Within the scope of these definitions, some state agencies and programs will be easier to classify than others. For example, state Medicaid programs must comply because they are considered health plans, as are health benefit plans for state employees. Academic medical centers and state mental hospitals are providers of care and are also subject to compliance.

Entities may also fall into more than one category. Some state Medicaid agencies may be considered both a health plan and a provider. The same may hold true for public health, substance abuse, social services, and other state authorities.

In the information age, however, institutions have come to rely on data from any number of interconnected sources to help carry-out their program objectives. Most health and human services agencies often interact with the same clients and depend on the same core group of safety net providers to fulfill their legal mandates. Data collected from these common providers and clients are used to determine provider reimbursement levels and client copays, coordinate client benefits, monitor program effectiveness, and secure grant funding and justify budget requests.

Beyond the explicit mandate HIPAA places on covered entities, compliance may also be required by agencies that are either exempt or not mentioned in the regulations.

---

**Covered Entities**

Under HIPAA, states have primary responsibility for determining which agencies and programs meet the definition(s) of a covered entity and are therefore subject to compliance. Among the programs and entities likely to be affected are:

- **Health plans**: Medicaid; State Children’s Health Insurance Program (SCHIP); state employee benefit programs; Temporary Assistance for Needy Families (TANF); and others.

- **Health care providers**: local health departments; community and migrant health centers; rural health clinics; school-based health centers; homeless clinics and shelters; public hospitals; maternal and child health programs (Title V); family planning programs (Title X); HIV/AIDS programs; and others.

- **Health information clearinghouses**: third-party administrators; pharmacy benefits managers; billing services; information management and technology vendors; and others.

A unique aspect of HIPAA is that it holds covered entities liable for the rule violations of their business associates, or those with whom they exchange information or contract for administrative and other services. Through trading partner agreements, covered entities are expected to reasonably ensure that their business associates are also HIPAA compliant.
Business Associates, Trading Partners, and the Ripple Effect
A unique aspect of HIPAA is that it holds covered entities liable for the rule violations of their business associates—those with whom they exchange information or contract for administrative and other services. This liability chain places extreme pressure on covered entities to reasonably ensure that anyone whom they share information or otherwise do business with is also HIPAA-compliant.

Through trading partner agreements, covered entities are expected to ensure that those with whom they share information are also HIPAA-compliant. Public health agencies, state budget offices, academic researchers, and others that rely on health information from covered entities will need to establish their own protocols ensuring that protected information is not used or accessed inappropriately. These business associates will also have to develop their technological capacity to collect, store, and transmit information in a “HIPAA-friendly” format and account for all any disclosures.

HIPAA does exempt certain transactions that address public health concerns, health care delivery and costs, and other issues. However, the new constraints HIPAA places on the exchangeable format of health information will undoubtedly affect the operations of many state programs that are either exempt or not expressly covered in the regulations (e.g., state controllers, state personnel boards, state retirement systems, and state finance departments, etc.). The effects of noncompliance can vary from civil and criminal penalties to potential lawsuits and operational disruption.

The Privacy Rule: Managing Liability
The major concern imposed on states by the privacy rule is liability. The privacy rule holds covered entities liable for the misuse or mishandling of protected health information. HHS’ Office of Civil Rights (OCR) is responsible for enforcing the privacy rule. Noncompliance can trigger civil fines of up to $100 per violation per person (up to $25,000 maximum). Individuals convicted of wrongfully disclosing protected health information can also face criminal fines of up to $250,000 and up to ten years in prison.

To comply with the privacy rule, covered entities must establish new protocols and procedures to ensure protected health information remains confidential. Unfortunately, different interpretations of the privacy rule have made it difficult to assess fully a state’s exposure to liability. Key among these interpretive issues are: the definition of protected health information; the conditions necessary for disclosure; and determining when certain standards should be governed by state law, HIPAA, or other federal privacy laws.

Defining protected health information. Despite its 367 pages, the privacy rule leaves open to interpretation the specific types of data elements, records, transactions, and entities that it covers. It defines individually identifiable health information generally as any information (including demographic information) collected from an individual that:

- is created or received by a health care provider, health plan, employer, or health care clearinghouse;
- relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and/or
identifies (or may be used to identify) the individual.

Beyond its broad definition, the privacy rule further empowers consumers to self-identify any information they themselves consider confidential. Covered entities must therefore take great care to identify any information that may be interpreted by consumers as an infringement on their right to privacy.

**Defining the standard for “minimum amount necessary.”** The privacy rule requires covered entities to keep to the minimum amount necessary the use and disclosure of protected health information. Covered entities must determine this threshold based on industry standards and their own professional judgment. While this broad guidance provides flexibility, it also leaves state and local policymakers at risk for failing to comply with the HIPAA privacy standards based on other interpretations of the “minimum amount necessary” standard.

**Determining when preemption applies.** The intent of HIPAA was to establish a floor of federal standards to protect the privacy of individually identifiable health information. Above this floor of federal protection, the privacy rule may be preempted by stronger privacy standards imposed by state law. Many states have already passed laws that to varying degrees protect patient privacy.

Determining which of these laws are “stronger” will require states to compare the relative strength of their privacy laws to HIPAA. Where a state law does not meet a particular federal standard, the privacy rule effectively preempts the existing state law. The state must then either enact stronger privacy standards or adopt those standards prescribed by the privacy rule to achieve HIPAA compliance.

The privacy rule may also be superseded by other federal privacy laws, thus requiring another assessment of which federal laws are applicable to states. The legal issues involved will make preemption determinations particularly challenging for those states that routinely share protected health information across state lines.

**Privacy Rule Changes**

On March 27, 2002, HHS proposed a number of changes to the “final” privacy rule. Among the changes proposed were:

- removing consent requirements that might adversely affect the delivery of health care.
- establishing model contract provisions for covered entities to use when securing business associate agreements.
- ensuring parental access to their children's health records based on state law.
- eliminating requirements to track disclosures for which a patient provided written consent.
- allowing covered entities to more easily share protected health information among themselves for treatment, payment, and other activities.

Prior to the proposed changes, states had already committed significant resources to comply with the privacy rule, which was finalized April 14, 2001. The effect these modifications will have on existing state compliance efforts will remain unclear until the proposed changes are finalized.

Under HIPAA, HHS can propose changes to any HIPAA rule (including the privacy rule) within one year of finalization without extending the compliance deadline. States and most other covered entities have until April 14, 2003, to achieve compliance with the privacy rule.

Kentucky, New York, North Carolina, Ohio, and other states have established workgroups to determine whether existing standards or requirements should be governed by state law, HIPAA, or other federal privacy laws. Most state legal workgroups include general counsels from the affected agencies and in some cases the state attorney general’s office.

Where questions remain, states may request OCR to determine whether certain standards or requirements should be governed by state or federal law. States may also request a waiver from certain standards or requirements imposed by the privacy rule. Such requests must be submitted in writing to OCR by the Governor or his or her designee.13

The option for states to meet or exceed the federal floor of HIPAA privacy protections applies only to the privacy rule. The electronic transactions and codes rule requires states to adopt the federal standard to perform certain administrative and financial transactions prescribed under HIPAA.

The Transactions and Codes Rule: Operational Challenges
Distinguishing the privacy rule from the electronic transactions and codes rule has been a major source of confusion under HIPAA. Both rules derive their statutory authority from Title II of HIPAA and they both apply to the same covered entities. But the implications of the rules on covered entities are quite different.

Where the privacy rule deals largely with issues of protocol and liability, the electronic transactions and codes rule focuses on the electronic exchange of protected health information. Through the transactions and code rule, HIPAA requires all covered entities to use a standard set of billing codes whenever conducting any of the following transactions electronically:

- health plan enrollment (or disenrollment);
- health plan eligibility determinations;
- health plan premium payments;
- first report of injury;
- referral certification and authorization;
- submission of claims and related encounter information;
- inclusion of claim attachments;14
- coordination of benefits;
- verification of claim status;
- issuance of payment and remittance advices; and
- other transactions that may be prescribed.

Operationally, covered entities—as well as business associates—will have to determine whether their current

<table>
<thead>
<tr>
<th>Transactions and Codes Deadline Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>On December 27, 2001, Congress passed the Administrative Simplification Compliance Act, which conditionally extended the deadline for covered entities to comply with the transactions and codes rule. States may obtain an additional year to comply with the transactions and codes rule by submitting a compliance plan to HHS before October 16, 2002, that includes the following:</td>
</tr>
<tr>
<td>• an explanation of why compliance could not be achieved by the original deadline;</td>
</tr>
<tr>
<td>• a budget, schedule, work plan, and implementation schedule for achieving compliance;</td>
</tr>
<tr>
<td>• an indication of whether a contractor or outside vendor will be used to help achieve compliance; and</td>
</tr>
<tr>
<td>• a testing schedule that begins prior to April 16, 2003.</td>
</tr>
<tr>
<td>Although a compliance plan must be submitted to obtain the one-year extension, there is no requirement that HHS approve the plan in order for the extension to apply. Small health plans are not eligible for the extension, and the extension only applies to the transactions and codes rule. States must still be in compliance with the privacy rule by April 2003.</td>
</tr>
<tr>
<td>Source: Public Law 107-105 (12/27/2001)</td>
</tr>
</tbody>
</table>
information systems will support the standardized electronic format required by HIPAA. HHS may impose civil fines of up to $100 per violation (up to $25,000 maximum) on individuals who conduct the above transactions in a nonstandard format.\textsuperscript{15}

**Technological capability.** Because the intent of the transactions and codes rule is to standardize the electronic exchange of health care information, covered entities will have to develop the technological capacity to exchange electronic information in a standardized (or HIPAA-friendly) format. As a result, covered entities must either:

- upgrade (or replace) their current information collection system to support the HIPAA-friendly format; or
- contract with a health information clearinghouse to translate HIPAA-friendly information into a usable format.

Supporting the new HIPAA-friendly format will also affect state authorities that routinely exchange information with covered entities, such as public health agencies, human services programs, criminal justice authorities, state budget offices, academic researchers, and others. To avoid service disruptions—paying providers, coordinating client benefits, managing patient care—affected programs must identify everywhere in their business process these electronic transactions occur and how they will be affected.

**Loss of local billing codes.** Over the years, state Medicaid agencies have created their own unique set of billing codes (called local codes) to facilitate provider billing, coordination of patient benefits, and the overall administration of their programs. The use of local billing codes has allowed states to enhance their Medicaid programs with eligibility expansions, benefit enhancements, and other unique features not offered under the traditional Medicaid program.

The transactions and codes rule requires all covered entities to abandon their use of local codes in favor of using a uniform set of national billing codes.\textsuperscript{16} State Medicaid programs in most cases will have to merge or “crosswalk” approximately 30,000 local codes into approximately 2000 national billing codes.

The elimination of local codes is certain to affect the operation of many innovative state Medicaid programs, particularly those operating under federal waivers that rely heavily on local codes to administer their programs. Combined with the creation of a national set of billing codes, the loss of local codes will require every state Medicaid agency to upgrade or replace its information system to maintain the new electronic transactions and codes standard.

**Compliance Strategies**

Determining which programs and policies will be impacted by HIPAA has been much debated among federal officials, state Medicaid directors, state attorneys-general, providers, consultants, and others. Still, absent federal guidance and without a precedent to follow, several states have embarked on coordinated, statewide campaigns to economize their HIPAA compliance activities. Common elements among these state efforts include:

- management by a state agency or other public entity with authority to coordinate the compliance efforts of impacted agencies;
- collaboration with a formal advisory group or steering committee (with representation from the offices of the Governor, state budget director, state chief information officer, attorney
general, directors and general counsel of the impacted agencies, city and county government officials, provider groups, third-party administrators, and others);

• an initial impact assessment to determine the level of statewide effort needed to comply;

• a formal, statewide implementation plan to guide compliance activities; and

• an implementation and testing schedule to ensure compliance is achieved with minimal disruption to impacted programs.

Legislation in California created the Office of HIPAA Implementation (CalOHI) to assume leadership for the state’s HIPAA activities. Housed in the California Health and Human Services Agency and supported by a steering committee of designated state agency HIPAA coordinators and county representatives, CalOHI’s charge includes:

• providing leadership and oversight for the efficient, effective and standardized HIPAA implementation by all agencies, departments, boards and commissions within the state government impacted by the HIPAA requirements;

• ensuring the state legislature and administration remain informed about the progress, issues, and risks facing impacted state entities;

• developing policies and procedures, and providing legal and technical advice (including education and training) for impacted state entities; and

• facilitating collaboration among federal, state, and county agencies, as well as private-sector health care entities, to resolve issues and minimize risks during HIPAA implementation.

Already, CalOHI has completed a statewide impact assessment and developed processes so agencies can report progress, execute contracts, and identify training opportunities. These processes include developing quarterly reports to identify progress and fiscal issues, developing master services agreements to help state agencies locate and secure contractors, and a training consortium with other western states.

An organizational outline of the California HIPAA statewide management structure is provided in Appendix B.

In North Carolina, language was included in the state budget for the Department of Health and Human Services (DHHS) to complete a high-level, statewide HIPAA impact assessment and compliance plan.

• **Clear authority.** With authority from the Governor, state agencies were contacted by the State Budget Officer and instructed to conduct organizational impact assessments through a Statewide HIPAA Assessment Team.

• **Centralized management.** The Statewide HIPAA Assessment Team is led by the same Program Management Office (PMO) leading the compliance efforts within DHHS. The PMO works with HIPAA coordinators in DHHS divisions to determine whether they would be impacted by HIPAA and, if so, to assess the level of effort needed to achieve compliance. As a separate activity, the PMO is also responsible for conducting a preliminary statewide
assessment for all state agencies, boards, commissions, community colleges, and the university system. Assessment results are to be documented in the statewide strategic plan for complying with HIPAA.

- **Coordinated action plan.** The state’s HIPAA Strategic Plan will report on the administrative systems, policies, and information systems throughout the state; establish a timeline for achieving compliance; and provide a cost-and-cash flow analysis for each state agency subject to compliance. The report will also outline personnel requirements, information technology equipment needs, and other operating and start-up expenses needed to comply with the HIPAA requirements.

The impact assessments already have been completed and the team now is compiling the results into a statewide compliance plan for the General Assembly. An outline of the state’s decision-making structure is provided in Appendix C.

The Governor’s Office in **Ohio** is sponsoring an effort (called an Engagement Management Structure) to strategically coordinate the efforts of state agencies affected by HIPAA’s administrative simplification requirements.

- **Collaborative leadership.** The Engagement Management Structure is led by an Executive Leadership Committee (ELC), comprised of a representative from the Governor’s office and directors from thirteen state agencies. The main priority of the ELC is to ensure that technical systems and business processes are integrated across state agencies and that the state achieves compliance with HIPAA. The ELC coordinates national and interagency compliance issues and secures the resources needed for compliance.

- **Coordinated management.** The project is managed by a Deputy Directors Project Management Team comprised of the deputy directors of the affected agencies. The deputy directors’ team coordinates and evaluates the policy recommendations of two committees (and several workgroups) comprised of policy and program experts from the affected agencies. The deputy directors team reports directly to the ELC.

- **Strategic expertise.** Two committees have been established to assist the Deputy Directors Project Management team: a Business Partners Committee and a Technology Partners Committee. The committees review the operational and technological issues to be resolved, form workgroups to help resolve those issues, and provide recommendations to Deputy Directors Project Management Team.

- **Technical expertise.** Several workgroups support the committees by helping to identify stakeholders, develop training tools, and establishing compliance standards. Currently, workgroups are established to address five HIPAA-specific issue areas: privacy, security, code sets, education, and agreements/legal contracts.

An organizational outline of the Engagement Management Structure is provided in Appendix D.

**Public-Private Collaboratives.** At least twelve state or regional public-private collaboratives have been created for affected entities to exchange ideas and resources to help them achieve HIPAA compliance. Among these collaboratives are the **Hawaii** HIPAA Readiness Collaborative, the **North Carolina** Healthcare Information and Communications Alliance (NCHICA), the Southern HIPAA Administrative Regional Process (SHARP), and the...


**Washington** State HIPAA Partnership. Additional information on various public-private collaboratives may be found in Appendix E.

**Impact assessment tools.** As compliance activities have continued, a number of states have developed assessment tools to help their agencies identify common challenges and avoid duplication of effort.

- **Cabinet-level awareness survey.** In Kentucky, the Governor’s Office for Technology (GOT) developed an online HIPAA compliance survey for state cabinet-level members. The survey was comprised of ten questions designed to assess each cabinet member’s level of knowledge about HIPAA and the impact it would have on their cabinet. The survey also sought to obtain estimated compliance costs and budget needs for each cabinet-level agency. A copy of the online survey is contained in Appendix F.

  Based on the results of the survey, the GOT is now coordinating a work group of affected agencies. The purpose of the work group is to develop common training tools and share HIPAA-related information. The work group will assist state agencies with a number of activities, including: conducting a HIPAA GAP analysis, developing business associate agreements, facilitating work with outside vendors, and building awareness among stakeholders.

- **HIPAA EarlyView™ Privacy.** In North Carolina, the Statewide HIPAA Assessment Team helped create HIPAA EarlyView™ Privacy, a self-assessment tool designed to help state agencies and other institutions determine the level of effort needed to comply with the privacy rule. A similar assessment tool is being developed to help organizations achieve compliance with the security rule.

- **A Guide to Privacy Readiness.** The Maryland Health Care Commission (MHCC) developed *A Guide to Privacy Readiness*, a self-assessment tool designed to help practitioners and small facilities complete their own privacy assessment. The guide also provides some industry-developed suggestions for meeting the compliance standards. Once completed, users will have a functional work plan to assist them in implementing the privacy standards. MHCC plans to issue a similar tool (*A Guide to Security Readiness*) in the summer of 2002.

  Additional state-developed assessment tools are listed in Appendix G.

**Conclusion**

It is likely that HIPAA-related compliance costs will exceed the approximately $3.5 billion incurred by states during the Y2K computing crisis.\(^\text{20}\) State agencies and programs will avoid sanctions only by establishing new policies and procedures to ensure individually identifiable health information is not misused or mishandled. In addition, they will avoid operational disruption only by developing their technological capacity to support the new, standardized format for exchanging electronic health information.

Achieving HIPAA compliance will require a labor-intensive review of how protected health information flows throughout state government. Even agencies that are exempt or not expressly covered by HIPAA will have to assess their reliance on protected information from covered entities and comply. Nevertheless, states are continuing to pursue innovative ways to minimize its fiscal and operational impact.


11 Among the federal laws that already govern privacy are the: Privacy Act of 1974; Freedom of Information Act; Employee Retirement Income Security Act of 1974 (ERISA); Family Educational Rights and Privacy Act; and Gramm-Leach-Bliley Financial Modernization Act.


13 It remains unclear whether the claims attachments standards will be governed under the current transactions and codes rule or adopted as a separate rule altogether.


APPENDIX A: Administrative Simplification At-A-Glance

Under HIPAA, administrative simplification is the common name given to seven different federal regulations being issued by the U.S. Department of Health and Human Services (HHS). Collectively these rules require all health plans, health care clearinghouses, and other health care providers to ensure that individually identifiable health information remains private and secure. They also require these covered entities (and their business associates) to standardize the way electronic administrative and financial health care data is exchanged. These rules include:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Purpose</th>
<th>Enforcement Agency</th>
<th>Proposed Rule</th>
<th>Final Rule</th>
<th>Compliance Deadline†</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Creates a floor of standards (procedures and protocols) to protect a patient’s right to keep their medical records and other personal health information confidential. The privacy rule outlines the procedures required for the exercise of those rights and the conditions necessary for others to use or disclose protected health information.</td>
<td>HHS Office of Civil Rights (OCR)</td>
<td>11/99</td>
<td>04/01‡</td>
<td>04/03</td>
</tr>
<tr>
<td>Security</td>
<td>Establishes minimum administrative, technical, and physical safeguard requirements to prevent unauthorized access to health information.</td>
<td>TBD</td>
<td>08/98</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Transactions and Codes</td>
<td>Establishes uniform standards to govern how certain treatment, billing, enrollment, and other health information must be formatted (codes) and exchanged (transactions) electronically.</td>
<td>Centers for Medicare and Medicaid Services (CMS)</td>
<td>05/98</td>
<td>10/00</td>
<td>10/02*</td>
</tr>
<tr>
<td>National Provider Identifier</td>
<td>Mandates the assignment of unique alphanumerics numbers to individually identify providers (or sellers) of health care services for billing and other purposes.</td>
<td>TBD</td>
<td>05/98</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Health Plan Identifier</td>
<td>Mandates the assignment of unique alphanumerics numbers to individually identify group plans providing health care benefits through insurance. Health plan identifiers are often used to enroll new employees; verify beneficiary (or employee) eligibility, benefits, and premium payments; and other purposes.</td>
<td>TBD</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Employer Identifier</td>
<td>Mandates the assignment of unique alphanumerics numbers to individually identify health plan sponsors (or employers). Employer identifiers are often used to enroll new employees; verify beneficiary (or employee) eligibility, benefits, and premium payments; and other purposes.</td>
<td>TBD</td>
<td>06/98</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Clarifies the framework for enforcing the administrative simplification regulations.</td>
<td>TBD</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

† Small health plans have one additional year following this date to be compliant.
‡ HHS proposed modifications to the privacy rule on March 27, 2002. The compliance deadline will not change.
* This deadline may be extended by one year if a compliance plan is submitted to HHS before October 16, 2002. Small health plans are not eligible for the conditional extension.
APPENDIX B

California Office of HIPAA Implementation

Governor

General Assembly (SB 456)

Other State Agencies

California Health and Human Services Agency

Office of HIPAA Implementation (CalOHI)

Statewide Workgroup

HIPAA Workgroups Steering Committee

Conceptual Workgroups
- Privacy
- Security
- Transactions
- Enterprise & Infrastructure
- Legal
- Communication
- Research
- Counties & State

Statutory Advisory Committee
- County Government
- Consumers
- Physicians & Surgeons
- Clinics
- Hospitals
- Pharmaceutical Companies
- Health Service Plans
- Disability Insurers
- Long-Term Care Facilities
- Mental Health Providers
- Other Stakeholders

Operational Support (Divisions)
- Policy Management
- Program Development
- Liaison, Technical Assistance & Training
- Planning & Reporting
- Operations
- Program Review
- Corrective Actions
- Business & Contractual Services
- Data Collection & Analysis
- Legal Counsel
- Information Technology
APPENDIX C

North Carolina HIPAA Program Management Office
(Department of Health and Human Services Only)

Governor

Department of Health & Human Services

DHHS Division of Information Resource Management

Oversight Committee (Division Directors)

DHHS HIPAA Program Management Office (PMO)

Designated HIPAA Coordinator(s) for DHHS Offices & Divisions

DHHS Division HIPAA Projects

North Carolina HIPAA Statewide Assessment Project
(For Agencies & Divisions Outside of DHHS)

Governor

General Assembly (SB 1005)

Other State Agencies

Office of State Budget & Management

Office of Information Technology Services

Department of Health & Human Services (DHHS)

Statewide HIPAA Assessment Project Manager

Other Agency Offices & Divisions (Designated HIPAA Coordinators)

Note: While North Carolina’s Statewide HIPAA Assessment Project is housed in the DHHS Program Management Office, it is managed separately from DHHS’ internal HIPAA compliance activities.
APPENDIX D

Ohio HIPAA Statewide Project
Engagement Management Structure

Governor

Executive Leadership Committee (ELC)
(Cabinet-Level)

Deputy Director Project Management Team (PM)
Governor’s Office
Department of Administrative Services
Department of Aging
Department of Alcohol and Drug Addiction Services
Department of Health
Department of Job and Family Services
Department of Mental Health
Department of Mental Retardation and Developmental Disabilities
Department of Rehabilitation and Corrections
Attorney General
Auditor of State
Office of Management and Budget
Bureau of Worker’s Compensation
Ohio Veterans Home

Business Partners Committee
(A committee of policy and program experts from the affected agencies)

Technology Partners Committee
(A committee of information technology experts from the affected agencies)

Privacy Workgroup
Security Workgroup
Code Sets Workgroup
Education Workgroup
Agreements/Contracts & Legal Workgroup
APPENDIX E

Public-Private Collaboratives

**Government Information Value Exchange for States (GIVES)** is a national collaborative focus group helping state agencies to meet the immediate need to exchange information, identify common government challenges, share solutions, and avoid duplication in order to attain HIPAA compliance within the timeframe required. ([http://www.hipaagives.org/](http://www.hipaagives.org/))

**Southern California HIPAA Forum** is a group of public and private healthcare organizations whose goal is to collaborate on approaches, techniques, and best practices for HIPAA compliance; discuss issues such as "gray areas" in the HIPAA regulations; and influence ongoing developments related to HIPAA. ([http://www.hipaausa.com/socal/forum.html](http://www.hipaausa.com/socal/forum.html))

**Hawaii HIPAA Readiness Collaborative** is an alliance of stakeholders in Hawaii seeking to realize the positive potential of HIPAA, including improving the flow of patient information to improve patient care and reducing administrative overhead. More immediate objectives relate to reducing HIPAA implementation costs by standardizing approaches, pooling resources and, potentially sharing consultant expenses. The Collaborative is part of the Hawaii Health Information Corporation, a private, nonprofit corporation whose mission is to collect, analyze and disseminate statewide health information and to support efforts to continuously improve the quality and cost-efficiency of Hawaii's health care services. ([http://www.hhic.org/hipaa](http://www.hhic.org/hipaa))

**Massachusetts Health Data Consortium** is a private, nonprofit consortium of public and private organizations whose mission is to develop, collect, analyze, and disseminate health care information to improve the health of New Englanders. ([http://www.mahealthdata.org/](http://www.mahealthdata.org/))

**Minnesota Center for Healthcare Electronic Commerce (MCHEC)** is a membership-driven organization whose purpose is to assist the health care industry in adopting standardized electronic commerce solutions to increase efficiency and provide better health care to patients. MCHEC is a committee of the Minnesota Health Data Institute, a nonprofit public-private partnership dedicated to measuring and improving the quality and efficiency of health care services in Minnesota. ([http://www.mhdi.org/mchec/index.html](http://www.mhdi.org/mchec/index.html))

**New England HIPAA Workgroup (NEHW)** is a regional group of public and private healthcare organizations whose goal is to share information and collaborate on HIPAA compliance. ([http://www.hipaausa.com/NEHW.html](http://www.hipaausa.com/NEHW.html))

**New Hampshire & Vermont Strategic HIPAA Implementation Plan (NHVSHIP)** is a volunteer organization of hospitals, physicians, other health care providers, health plans, state health departments, and vendors whose goal is to promote compliance and understanding of all aspects of HIPAA. ([http://www.nhvship.org/](http://www.nhvship.org/))

**North Carolina Healthcare Information and Communications Alliance (NCHICA)** is a nonprofit consortium of providers, payers, corporate partners, professional associations, and government agencies dedicated to improving healthcare through information technology and secure communications. ([http://www.nchica.org/](http://www.nchica.org/))
**e-Pennsylvania Alliance** is a nonprofit organization whose mission is to identify and study public issues in communications and information technologies and to suggest strategies for the future consideration and implementations. Its members represent business, industry, government, education, health, libraries, arts, nonprofit and trade associations. ([http://www.e-paalliance.org/](http://www.e-paalliance.org/))

**Southern HIPAA Administrative Regional Process (SHARP)** is a nonprofit, public-private workgroup established to meet the immediate need of assessing regional HIPAA Administrative Simplification implementation readiness to bring about regional coordination for successful HIPAA compliance by all stakeholders in the southern regional healthcare industry. ([http://www.sharpworkgroup.com](http://www.sharpworkgroup.com))

**Utah Health Information Network** is a broad based coalition of insurers, providers and other interested parties, including State government, who have come together for the common goal of reducing health care administrative costs through standardization and electronic data interchange (EDI) of health data. ([http://www.uhin.com/](http://www.uhin.com/))

**Washington State HIPAA Partnership** is a collaboration of state and local government officials and others who are working on HIPAA readiness. The Partnership’s mission is to share information, expertise and compliance strategies. ([http://maa.dshs.wa.gov/dshshipaa/](http://maa.dshs.wa.gov/dshshipaa/))

**HIPAA Collaborative of Wisconsin (COW)** is a non-profit organization real or potential covered entities, business associates, and/or trading partners under HIPAA, as well as any other organization impacted by HIPAA regulation. The mission of HIPAA-COW is to create consistency among payers and providers regarding HIPAA implementation; develop a common HIPAA implementation vision; facilitate and streamline HIPAA implementation through identification of “best practices” and benchmarking; reduce duplicative efforts among payers and providers; offer opportunities for partnering; and identify and elevate regulatory issues to state agencies and the legislature. ([http://www.hipaacow.org/](http://www.hipaacow.org/))
### APPENDIX F

#### Kentucky Cabinet-Level Awareness Survey

1. Please select your cabinet/agency:  
   (Click here to choose)

2. Will HIPAA impact the business processes, data, or IT systems in your Cabinet?  
   - Yes  
   - No  
   - Don’t Know

   **If Yes, please answer the following:**

3. Which agencies in your Cabinet will be most affected?

4. Assess your agency’s HIPAA compliance status:  
   - Cabinet/Department is not aware of HIPAA requirements.  
   - Cabinet/Department is aware of HIPAA. Some preliminary assessment has taken place.  
   - Cabinet/Department is actively changing business processes and IT systems to meet HIPAA requirements.  
   - Cabinet/Department has completed HIPAA compliance activities and actively monitors Federal regulation development.

5. What do you estimate the total cost and time required to achieve HIPAA compliance in your Cabinet?  
   - $  
   - months

6. Are these funds included in your current budget?  
   - No  
   - Yes ... How Much $  

7. Are these funds expected to be requested in the FY2003-FY2005 biennial budget?  
   - No  
   - Yes ... How Much $  

8. Please identify your HIPAA coordinator or manager:  
   - Name  
   - Address  
   - Phone number

[Click to SubmitHIPAA]
APPENDIX G

State-Developed Compliance Tools

Cabinet-Level Impact Awareness Survey (Kentucky Governor’s Office for Technology) is designed to assess each cabinet member’s level of knowledge about HIPAA and how their cabinet would be impacted. The survey also seeks to obtain estimated compliance costs and budget needs for each cabinet-level agency.

Statewide Business Information Flow Assessment (North Carolina Department of Health and Human Services) is designed to help state agencies compare their current operations to HIPAA requirements. Specifically, the tool helps state agencies to assess their current business operations, the flow of health information into and out of their agencies, and the flow (and handling) of information within their agency including security practices.

Electronic Data Interchange (EDI) Assessment (North Carolina Department of Health and Human Services) is designed to help states evaluate the impact of HIPAA's transaction, code set, and identifier regulations on divisions within a state agency. It includes a questionnaire to help assess the capacity of current information systems to function in a “HIPAA friendly” environment.

Electronic Data Interchange (EDI) Assessment Tool (Ohio HIPAA Statewide Project) is designed to help states evaluate the impact of HIPAA's transaction, code set, and identifier regulations on divisions within a state agency.

Covered Entity Screening Tool (Ohio HIPAA Statewide Project) helps state agencies self-assess whether or not they may be a covered entity, hybrid entity, or not affected by HIPAA.

HIPAA Impact Assessment Tool (New York Office for Technology) helps state agencies self-assess whether or not they may be a covered entity, hybrid entity, or not affected by HIPAA.

HIPAA Awareness Self-Assessment Checklist (Washington State HIPAA Partnership) is a voluntary survey to help providers establish a baseline for the level of effort needed to achieve HIPAA compliance.

Model Business Associate Agreement (Ohio HIPAA Statewide Project) provides guidance to state agencies on how to develop business associate agreements.

HIPAA Facilities Checklist (California Department of Health Services). This checklist is meant to help facilities, agency staff, and management to determine their technical readiness for HIPAA.

A Guide to Privacy Readiness (Maryland Health Care Commission) is intended to assist most practitioners and small facilities in their privacy assessment, and to provide some industry-developed suggestions for meeting the compliance standards. At the completion of the self-assessment, users will have a functional work plan to assist them in implementing the Privacy Standards. HIPAA is intended to be scalable, users of this guide are encouraged to implement the HIPAA requirements in a manner consistent with their organization’s size.

Maryland Health Care Commission Privacy
HIPAA EarlyView Privacy™ (North Carolina Healthcare Information and Communications Alliance) was designed to help healthcare organizations engaged in compliance initiatives assess their current state of HIPAA-readiness, identify needed tasks, and prepare key compliance documents.

HIPAA EarlyView Security™ (North Carolina Healthcare Information and Communications Alliance, Inc.) is intended for health plans, provider organizations, clearinghouses, and public agencies. It has been designed to provide an overview of an organization's current status relative to the implementation requirements in the proposed HIPAA Security Regulations. Reports generated through the use of this tool may provide useful guidance to an organization in formulating an appropriate response.