An LAO Report

Health Insurance Portability and Accountability Act

Issue

Compliance with the federal Health Insurance Portability and Accountability Act (HIPAA) will require the health care industry to change processes and systems that will result in significant costs.

LAO Findings

The state has initiated significant efforts to comply with HIPAA. However, based on lessons learned during the state's Year 2000 (Y2K) compliance efforts, we conclude that the administration's approach has some weaknesses. For example, a lead agency has not been designated to oversee HIPAA activities and ensure that affected departments participate in compliance efforts. Nor has a comprehensive statewide plan been developed to address HIPAA compliance activities, which could mean these efforts will not be well coordinated, consistent, and complete. Additionally, few departments have assessed the likely impact of HIPAA on their operations. Consequently, they may lack a full understanding of the necessary compliance efforts, funding requirements, and time to complete their efforts.

The *2001-02 Governor's Budget* plan lacks the statutory framework that is needed for such a broad and complex endeavor. Moreover, the budget proposes a fragmented funding process that could result in confusion because of a split in approval authority.

LAO Recommendations

We recommend the enactment of state legislation providing an appropriate policy framework to govern HIPAA compliance activities. This legislation should include specific provisions that designate the Health and Human Services Agency (HHSA) as the lead agency, direct HHSA to develop a statewide HIPAA plan, require departments to complete assessments, and establish clear lines of authority over the administration of the fund. The administration's budget bill language would be replaced with language that makes HIPAA allocations subject to the proposed legislation.

To improve oversight, we recommend that the Legislature approve the funding requested in the 2001-02 budget for HIPAA activities, but schedule the requested funds in the proposed new budget item (9909). We also recommend that positions requested by departments for HIPAA compliance activities be limited to two-year term positions.

Elizabeth G. Hill
Legislative Analyst

March 27, 2001

BACKGROUND

Governor's Budget Requests. The *2001-02 Governor's Budget* requests a total of $92 million ($23.6 million General Fund) for statewide planning and implementation of the federal Health Insurance Portability and Accountability Act (HIPAA). This includes $70 million ($20 million General Fund) to be allocated to state departments and agencies that apply for funding. In addition, the budget provides about $22 million ($3.6 million General Fund) and 28 positions in four departments. In the following pages, we summarize the requirements of the act, analyze the potential effects on state and county governments, evaluate the approach taken to date by state agencies to comply with the law, and recommend further legislative actions that would improve the state's compliance.

What Is HIPAA? The HIPAA was enacted in 1996 and set many goals for the health care industry. The law's primary purpose was to protect health insurance coverage for workers and their families when they change or lose jobs. This new protection will impose additional administrative requirements on the health care industry. However, a section of the law requiring administrative simplification is designed to reduce these burdens. The general approach is to accelerate the move from paper based to electronic transactions through the establishment of national standards and requirements for the transmission, storage, and handling of certain electronic health care data.

Many experts believe that HIPAA is the most sweeping government action affecting the health care industry since the introduction of Medicare. They predict that HIPAA will affect nearly every business process of the health insurance industry and result in significant systems changes. Like efforts to address the Year 2000 (Y2K) technology problem, HIPAA does require changes in information technology (IT) systems, but HIPAA involves much more than IT projects. It will also affect administrative policies and regulations, operational processes, education, and training and these in turn will result in significant costs.

Who Must Comply? Both private and public sector organizations that provide health care services and use patient or other health care data must comply with HIPAA. Thus, the list of affected organizations includes not only health care providers, but also employers, insurers, and health plans. Health plans include Medicaid programs, Medicare, and most government-funded health care programs. The HIPAA will also affect state departments that are not considered to be health-related departments, but departments that may indirectly handle health care data such as the California Department of Veterans Affairs or the Public Employees' Retirement System (PERS). While HIPAA will affect both private and public organizations, our report focuses on the potential effects on state and county government.

In California, a number of state departments have recognized the potential impact of HIPAA's requirements and are participating in statewide compliance efforts. However, few departments have begun actual implementation work, such as developing a work plan. Some departments that may be affected do not appear to be participating in any compliance efforts. Figure 1 provides an overview of some departments which reported progress on HIPAA implementation as of October 2000. At this time, the state does not have a comprehensive list of all the departments that will be affected by HIPAA.

One of the departments that will be most significantly affected is the Department of Health Services (DHS). The DHS programs that have already been determined to be affected include Medi-Cal, Primary Care and Family Health, the Cancer Detection Section, the Information Technology Services Division, the Genetic Disease Branch, Children's Medical Services, and the Cancer Control Branch. Other departments that may be affected, but have not yet reported progress on HIPAA, include PERS, the Department of Rehabilitation, the State Teachers' Retirement System, the Department of Managed Health Care, and the Managed Risk Medical Insurance Board.

In addition to state departments, county health-related programs, including county medical services and county hospital and health systems that serve in the role as health care providers, have compliance obligations. Some of the county program areas known to be affected include mental health, Medi-Cal and Healthy Families eligibility, and California Children's Services.

Figure 1

Departments Reporting Progress on HIPAA Implementation as of October 2000

(In Thousands)

Departments	Developed a Work Plan	Inventory Assessment	Impact Analysis	Estimate of Total Cost[a]
Alcohol and Drug Programs	In development	No	No	$12,413
Board of Equalization	Started	Started	—	356
Aging	—[b]	—	—	364
Corrections	No	No	No	—
Highway Patrol	No	No	No	—
Youth Authority	No	No	No	—
Developmental Services	Yes	Yes	Yes	5,516
Health Services	Yes	Yes	Yes	100,000
Mental Health	Yes	Yes	Yes	23,936
Motor Vehicles	No	No	No	—
Rehabilitation	No	No	No	—
Emergency Medical Services Authority	No	Yes	Yes	421
Office of Statewide Health Planning and Development	In development	Yes	Yes	927
Total				**$143,933**

[a] Cost includes multiyear amounts.
[b] No information provided.

Benefits of Administrative Simplification. The administrative simplification component of HIPAA requires that all organizations that engage in the electronic transmission of administrative and financial health care information shall use a single set of electronic standards to submit and

receive claims, authorize referrals for medical services, enroll beneficiaries, and receive payments. Some of the benefits that may result from administrative simplification include:

- ***Increased Efficiency and Reduced Administrative Costs.*** The federal Health Care Financing Administration (HCFA) predicts that the health care industry will save about $1 billion during the first five years of HIPAA implementation. Others have estimated that billions of dollars will be saved each year by switching from paper claims to uniform electronic claims submission and using uniform billing requirements. We have not conducted our own analysis of the accuracy of these savings projections.

- ***Improved Effectiveness of the Health Care Industry.*** The standardization of information will enable the health care industry to take advantage of technical solutions to improve the overall effectiveness of the health care delivery system. For example, health care providers may be able to improve the management of their medical practices because they will be able to verify patient eligibility for medical services more quickly.

- ***Compare and Analyze Data.*** Currently, due to the pervasive use of local codes used to support special state health care programs, state Medicaid programs cannot compare data. With standardized codes, programs could analyze data that may allow them to identify relatively high-cost areas and more accurately evaluate which services and programs are most effective.

- ***Better Health Care for Beneficiaries.*** With the implementation of HIPAA, health care beneficiaries will find it easier for them, and their health records, to move to a new provider or health care plan (this is called "portability"). They will potentially benefit from improved continuity of health insurance coverage in groups and individual markets and greater coordination of care.

- ***Reduced Fraud and Abuse.*** Having a single set of unique identification numbers for specific providers, insurers, and patients should make it easier for authorities to detect medical fraud, waste, and abuse by eliminating situations where providers and individuals have multiple identifiers. These multiple identifiers make it difficult to match and track claims to both providers and individuals, particularly where fraud is intended.

What Are the Administrative Simplification Standards? To achieve administrative simplification the federal Department of Health and Human Services (HHS) as directed by the Act is developing standards that involve the following:

- ***Transaction Standards.*** The HHS has developed national standards designed to allow the electronic exchange of specific health care transactions. This includes standards for the transmission of claims for payment of medical services, enrollment in health plans, inquiries about patients' eligibility for services, and other critical health-related business transactions.

- ***Code Sets.*** These codes will standardize certain types of health care information such as diseases, injuries, impairments, and procedures on a national level.

- ***Unique Identifiers***. The HIPAA requires the adoption of unique identifier codes for health care plans, health care providers, and employers. For example, the identification number being proposed for employers is the Employer Identification Number which is issued and maintained by the Internal Revenue Service. Currently, employers may use different identification numbers when they conduct business which slows activities such as health plan enrollments and premium payments, and increases costs.

- ***System and Patient Data Security.*** Under HIPAA, security standards must be adopted that carry out "reasonable and appropriate" administrative procedures and safeguards to ensure the integrity and confidentiality of information. These rules require that certain entities enter into agreements that ensure that when an individual's information is transferred the information is protected in accordance with HIPAA's privacy and security rules.

- ***Privacy Standards.*** The privacy standards are intended to protect and enhance the rights of consumers, ensure the integrity of the health care system, and create a national framework for health privacy protection. The rule provides standards for covered information, entities, and disclosures.

When Must Organizations Comply? The HHS is planning on issuing rules for implementing HIPAA in stages or "waves." Under this approach, HHS will publish the proposed rules, receive and review comments on the rules and then will issue the finalized rules. This will allow HHS to respond to the large number of comments received. For example, more than 17,000 public comments were received on the proposed rules for transaction standards and code sets.

The first set of final standards, relating to transactions and code sets, published in August 2000, provide the health care industry until October 16, 2002, or about two years, to comply. The second set of standards released relate to privacy and the expected date of compliance for these rules is February 26, 2003. It is anticipated that the states can expect at least seven more waves of HIPAA regulations which will be issued

during the next two years, with each allowing roughly 24 months for implementation. These seven standards include national provider identifiers, national employer identifiers, security, national health plan identifiers, claims attachments, enforcement, and the national individual identifiers.

ORGANIZATIONAL CHALLENGES POSED BY HIPAA

Government organizations will encounter many challenges to comply with HIPAA. This will require organizations to make programmatic changes such as altering business processes, adapting to the loss of "local codes" that track the health care needs of specific groups, and modifying practices to ensure patient privacy.

The HIPAA Will Affect State and County Business Processes. The administrative simplification requirements of HIPAA will have a significant effect on the health care-related business processes of most state and local agencies because they do not currently conform with the majority of the proposed standards. Specific business processes that will be affected include billing and payment for health care services; the exchange of eligibility and enrollment information among health care providers, plans, and insurers; and referral and authorization processes for medical services. In addition, all government rules and regulations related to privacy and security policies, processes, and procedures will need to be changed significantly in order to achieve compliance.

The Loss of Local Codes Will Have a Significant Effect. The health coverage provided under state Medicaid programs can vary significantly in scope from coverage offered by other public- and private-sector health plans. Thus, some services provided under Medicaid may not generally be recognized by other health care payers and providers. Most state Medicaid agencies have created local codes (unique state and local identifiers) for identifying and tracking procedures, drugs, provider types, and categories of service. These codes enable Medicaid agencies to process claims for health care services that they provide to specific local populations of beneficiaries. Nationally, more than 22 categories of codes with additional individual codes have been identified for services including private nursing, mental health, and free immunizations for children.

Under HIPAA, a code set is any set of codes used for encoding data, such as medical diagnosis codes or medical procedure codes. The HHS-approved HIPAA code sets cover a range of medical conditions, such as diseases and injuries, or drugs and medical procedures. The HIPAA administrative simplification standards eliminate the use of local codes and require a switch to the HHS-approved code sets.

The elimination of local codes has programmatic implications that will affect information services, administrative policies and regulations, provider reimbursement levels, and oversight activities. The more local codes a state uses, the more policy and business decisions that will have

to be made to address such issues. Each of the nearly 1,100 local codes that are used to administratively support many special programs in California are written into state regulations and will need to be changed to eliminate the use of these nonstandard codes.

Reimbursement levels for services could also be affected by the loss of local codes. In order to comply with HIPAA, the state may have to "roll up" services to a level that could be more costly to the state and may result in California having to pay higher reimbursement rates. For example, a local code used to provide a specific type of mental health service to disabled children under age five may not be recognized by the national code system. Under HIPAA, the local code for those services may have to be rolled up to a code that generally covers mental health services for all children ages 1 through 18 and the reimbursement level for that code may be greater or less than the reimbursement rate for the local code.

Complying With Privacy Requirements. The recently released privacy requirements have the potential to significantly change business practices for both health care providers and insurers. The new privacy rules mandate that entities that collect health care information advise patients of their right to privacy and advise them about how their personal medical information might be used by entities that have access to the information. The rules also establish policies that allow patients to review, copy, and make corrections to their personal health information. Organizations may require extensive training to meet these requirements.

The State Will Have to Develop Comprehensive Policies to Satisfy Security Requirements. Every entity that handles health care information will be required by HIPAA to develop comprehensive policies for the security of that data. This involves nontechnological issues such as employee training, disaster-recovery planning, internal audits, and provider contracting, in addition to the technical security issues such as encryption of data.

MAJOR FISCAL ISSUES

Compliance with HIPAA is expected to have a significant fiscal impact nationwide. Estimates of compliance costs vary widely and the state has made an early estimate that compliance for just departments within the Health and Human Services Agency (HHSA) may cost more than $100 million over many years.

Complying With HIPAA Will Be Expensive. The HIPAA planning and implementation is

expected to have a major fiscal impact on the state because of the additional staff and funding necessary to analyze and change current operations, policies, and systems. Estimates of the cost to implement HIPAA vary widely, however. The U.S. Office of Management and Budget has estimated HIPAA implementation will cost the entire health care industry (both public and private sectors) approximately $3.8 billion over five years. Others have reported that industry-wide costs could go as high as $43 billion for the same time period. Rough estimates for an organization's costs range from one and one-half times to twice the cost of Y2K.

Several state Medicaid agencies have estimated the cost of complying with HIPAA. Their estimates range from $105 million in Texas (with annual Medicaid expenditures of $6 billion) to $18 million in Florida (with annual Medicaid expenditures of $7.5 billion). By way of comparison, California has annual Medicaid expenditures through the Medi-Cal program of $24.6 billion in the current fiscal year.

The cost of HIPAA will depend on the strategy taken for achieving compliance. For example, many state Medicaid agencies are reporting that they plan to replace their information systems as part of their implementation of HIPAA, thereby significantly increasing costs. Other factors affecting costs are the start-up costs of automation, training and process reengineering, and any costs associated with addressing implementation problems. Finally, we would note that much of the cost of implementing the new standards is likely to involve one-time expenditures.

Early Estimates of State Costs. In California, several state departments have begun estimating the cost of implementing HIPAA and have requested funding for the budget year totaling $22 million ($3.6 million General Fund). Other departments that may be impacted by HIPAA either have not requested funding or may not have estimated the cost of compliance.

Representatives of the state HHSA estimate that, agency-wide, compliance with HIPAA may cost more than $100 million over many years. This is an early estimate and most likely will change significantly because some departments and program areas have not been thoroughly assessed. Figure 1 (shown earlier) shows the steps that some departments have taken towards complying with HIPAA and preliminary cost estimates.

Federal Funding Is Available for Medi-Cal Compliance. Compliance with HIPAA standards is a federal mandate and, as such, HCFA has authorized the use of enhanced federal funds at the 90 percent match rate. These funds can be used for costs associated with the planning, design, development, and implementation of HIPAA requirements for the California Medicaid Management Information System (CA-MMIS) and related computer systems. The CA-MMIS is the medical and dental claims processing system used by DHS for various programs, including the Medi-Cal Program. Other information systems not related

to the CA-MMIS are eligible for claiming the normal federal Medi-Cal match of about 51 percent. The availability of federal funding means that state compliance costs will be much lower than would otherwise be the case.

Federal Funds Not Available for Non-Medicaid Programs. While HIPAA is a federal mandate, federal funds are not available for non-Medicaid-related programs. Costs associated with HIPAA project planning, assessment, and remediation for nonmedical programs (for example, the Department of Motor Vehicles) must be funded by the applicable funding source for the affected program.

Similarly, federal funding is not available for counties' compliance with HIPAA, even though counties may also incur significant costs due to the required conversion of local health service codes to national codes. Because local coding is largely related to the Medi-Cal program, the state will need to make decisions as to whether it will pay for any of the counties' cost of compliance. If the state decides to pay for some of the cost, this will increase the state's overall costs for HIPAA compliance.

Health care providers that the state contracts with for health care services must also comply with HIPAA. The state must determine if it will share in the cost of changes required by the 90,000 providers.

Risks From Failure to Meet HIPAA Requirements. Failure to comply with HIPAA could result in inefficiencies in the health care delivery system and have a significant fiscal impact on the state. Specifically, the state's failure to adopt the national standards would mean that the state could risk service interruptions of its major health programs, such as delays or an inability to process provider claims for payment. The state's ability to interact with business partners could also be hindered and leave the state unprepared for future transaction standards.

Failure to meet HIPAA requirements poses other fiscal risks as well. For example, it could result in the imposition of significant federal monetary penalties against the state and potentially even the loss of billions of dollars in federal reimbursements for its health programs. At the time this report was prepared, HCFA had proposed noncompliance fines of $25,000 a day, per data element, per transaction. The state might also be subject to costly litigation by not complying with HIPAA standards.

WHAT IS THE STATE CURRENTLY DOING?

The 2001-02 spending plan provides about $92 million ($23.6 million General Fund) in various budget items for HIPAA compliance activities. The DHS has established a HIPAA Project Office to act as a resource to guide and monitor compliance efforts. Other health-related departments have also begun compliance work and a separate budget item has been proposed to

provide allocations of funding to other departments for HIPAA-related activities.

The *2001-02 Governor's Budget* provides $23.6 million from the General Fund and about $69 million from other funds—roughly $92 million in all—for HIPAA compliance activities in the budget year. A number of compliance efforts are already under way. We discuss these activities in more detail below.

The DHS Has Leading State Role. As the agency overseeing the Medi-Cal and Healthy Families Programs, DHS is the largest purchaser of health care services within the state. For many "safety-net" providers such as County Organized Health Systems, DHS is the primary source of revenue. As the largest purchaser, DHS could greatly influence the rest of the California health care industry's compliance with HIPAA requirements.

The DHS received seven two-year limited-term positions in the *2000-01 Budget Act* to form a project work group to review and analyze final regulations, specify the effect on DHS programs, and develop a work plan for HIPAA compliance. In May 2000, DHS established the HIPAA Project Office and began performing initial HIPAA assessments of DHS programs, forming workgroups and participating in national groups focusing on standards, implementation, and legislation.

The Governor's budget requests, for the current fiscal year, to (1) administratively establish 11 additional positions beyond the 7 authorized in the *2000-01 Budget Act* to conduct rate studies, perform impact assessments, and participate in project planning and (2) increase federal funds by $1.2 million. As shown in Figure 2, for the budget year, the DHS budget requests $2 million from the General Fund for continuation of these 11 positions, 4 additional positions that would first be established in 2001-02, and consulting services. The DHS indicates that it may request during spring 2001 additional funding for the budget year based on impact assessments and the release of the final HIPAA rules.

So far, the HIPAA Project Office has completed initial assessments in nine program areas and

Figure 2

Budget Requests for HIPAA-Related Activities

(Dollars in Thousands)

	2001-02			
	Personnel Years	General Fund	Other Funds	Total Funds
Department of Health Services	15[a]	$2,000	$17,000	$19,000
Department of Mental Health	9	1,200	1,200	$2,400
Department of Developmental Services	3	425	425	$850
Office of Statewide Health Planning and Development	1	—	80	80
Health Insurance Portability and Accountability Act Fund (Item 9909)	—	20,000	50,000	70,000
Totals	**28**	**$23,625**	**$68,705**	**$92,330**

[a] Health Services received seven two-year limited-term positions and $585,000 ($260,000 General Fund) in the *2000-01 Budget Act* for HIPAA activities.

remediation has started on the Medi-Cal and Denti-Cal claims processing systems. The office has also begun to match local codes to national standards. Acting as a lead organization, DHS has given presentations and provided training in the past year to state departments, county organizations, and managed care groups and plans to present its approach to HIPAA as a model for other departments. However, the Project Office has emphasized that DHS program areas, other departments, and individual providers are responsible for their own HIPAA-related activities.

Department of Developmental Services (DDS). The DDS received a 2000-01 appropriation of $205,000 from the General Fund and three limited-term positions for the purpose of determining the impact of HIPAA. The budget for 2001-02 requests $850,000 ($425,000 General Fund and $425,000 in reimbursements) to comply with HIPAA's transactions and code sets requirements. The DDS is completing an initial analysis of the impact of these requirements on the department's Cost Recovery System (CRS) and on other IT systems. The CRS processes electronic billings to private insurance companies and claims to Medicare and Medicaid. The department plans to submit a feasibility study report this spring along with a Department of Finance (DOF) letter requesting additional funds once these initial assessments are completed. Later this spring, the department plans to address the impact of HIPAA on the business processes of the department, the developmental centers, the regional centers, and service providers.

Department of Mental Health. The Department of Mental Health (DMH) has completed a feasibility study report for compliance with the first wave of HIPAA regulations. The 2001-02 budget requests $2.4 million ($1.2 million General Fund and $1.2 million in reimbursements) and nine positions. The DMH is also establishing a special internal team to manage compliance activities in all four of its divisions and anticipates that the compliance effort will take five and one-half years.

Office of Statewide Health Planning and Development (OSHPD). The OSHPD 2001-02 budget requests one permanent full-time program position to evaluate the new HIPAA provisions and implement measures to comply with the data transaction and privacy standards. It is anticipated that by taking these steps the office will be able to protect the identity of individual patients.

The HIPAA Fund. The administration's 2001-02 budget proposal would establish a HIPAA fund—a separate budget item with a total of $70 million ($20 million General Fund, $10 million special funds, and $40 million nongovernmental cost funds)—to provide allocations to other departments for HIPAA compliance activities. To obtain funding, a department would submit a request to the DOF for HIPAA-related activities that the department could not fund with existing re-

sources. The DOF would review the funding request, and, if it agreed, would provide a 30-day notification to the Legislature that it intended to make an allocation from the HIPAA fund. If a HIPAA compliance activity included changes to an IT system, departments would also need approval from the Department of Information Technology (DOIT) prior to DOF notifying the Legislature of the allocation of funds.

WEAKNESSES IN THE ADMINISTRATION'S APPROACH

The state has initiated significant efforts to comply with HIPAA. However, based upon the lessons learned during the state's Y2K compliance efforts, we believe that the administration's approach has a number of weaknesses that we discuss below.

Our analysis indicates that the efforts initiated to date by state agencies to comply with the requirements of HIPAA are warranted and generally appropriate. However, based on lessons learned in previous efforts to address the Y2K problem, we believe there are several weaknesses in the state's current approach to addressing the challenges posed by HIPAA. We discuss several such concerns below.

Lack of Lead Agency. When a statewide program implementation effort is necessary, the state has sometimes designated a lead agency that is responsible for overseeing all related activities and ensuring that all departments that may be affected are participating in compliance activities. For example, the state's Y2K efforts were led by DOIT, which monitored all Y2K activities and reported to the Governor and Legislature on the state's overall progress. We believe this organizational strategy especially makes sense in situations when the task is complex and involves many different state agencies.

The HIPAA appears to be just a situation. While DHS has established the HIPAA Project Office to oversee and coordinate its own internal department efforts, the administration had not designated a lead agency for statewide HIPAA compliance activities at the time this report was prepared. Unless statewide project oversight responsibility is established, it may be difficult later to hold departments (including nonhealth departments) accountable for their efforts to comply with HIPAA.

Absence of a Statewide Plan. Comprehensive planning is another critical element for complex statewide projects. For example, in managing its Y2K efforts, the state developed a statewide Y2K plan which included the following components:

- A strategy for addressing the Y2K issue.
- Y2K remediation activities required for each department.
- Y2K oversight activities to be provided by DOIT.

- A common definition that the administration and the Legislature could use to determine when the state remediation activities were "complete."

At the time this report was prepared, however, the administration had not yet developed a statewide plan for addressing HIPAA compliance. Lacking such a statewide plan, HIPAA efforts may not be well-coordinated, consistent, and complete.

Lack of HIPAA Impact Assessments. Another important lesson the state learned from Y2K was the need for all departments to assess which IT systems would require Y2K remediation. These assessments formed the basis for department work plans and funding requests. Conducting assessments is an important planning component because it defines the scope of the effort, determines funding needs, and establishes time frames for completion of tasks.

At the time that this report was prepared, however, few departments within HHSA had begun assessments. Because of this lack of completed assessments, it is likely that departments do not have a full understanding of:

- The scope of their individual HIPAA compliance efforts.
- Their overall funding needs.
- The time frames needed to complete compliance activities.

Difficult to Administer Fund. The state encountered some difficulties in the administration of the Y2K fund. For example, DOIT and DOF sometimes took up to six months to review and approve requests for fund allocations. This caused some departments to have to delay starting Y2K remediation tasks and, as a result, these departments later had to devote *more* resources to compliance activities to make up for the lost time.

Another difficulty was the confusion between the role of DOIT and DOF in determining what constituted an appropriate expenditure from the Y2K Fund. On some occasions DOIT and DOF disagreed over what activities *should* and *should not* be funded through the Y2K Fund. We are concerned that this same problem could affect the administration of the HIPAA fund, given budget language that again splits the approval authority for IT activities between DOIT and DOF.

Weaknesses in Funding Mechanism Oversight. During the nine months leading up to the December 1999 deadline for Y2K compliance, a number of funding notifications received by the Legislature were to backfill for funds that had already been spent for Y2K efforts without prior legislative authorization. We are concerned that the notification mechanism proposed for the HIPAA fund would also result in broad administrative control over monies with limited opportunity for legislative review and oversight.

In addition, a number of the HIPAA requests propose to establish permanent positions. Establishing permanent positions for a time-limited task will limit the Legislature's ability to determine if the positions are still needed once HIPAA activities are complete.

Fragmented Funding Processes. The budget proposes to fund specific HIPAA-related activities in four separate departmental budget items. In addition, it provides funding for unspecified activities through the HIPAA fund. In effect, the administration is using two processes to fund similar activities. Over time, this approach could become a problem when the Legislature tries to determine the total cost for HIPAA compliance. This problem occurred with Y2K remediation when the administration allocated funds to individual departments through the annual budget process in addition to funding the Y2K fund. The Legislature was not able to determine the state's total spending on Y2K remediation.

Lack of Statutory Framework. The state's Y2K remediation activities, unlike those for HIPAA, were limited to a single set of activities that were well-defined beforehand, consistent throughout government and private industry, and focused exclusively on IT systems. The HIPAA compliance activities, on the other hand, are much broader in scope—encompassing mainly changes in administrative policies and regulation as well as some changes to IT systems. The Governor's budget plan does not offer a statutory framework for the HIPAA statutory compliance program except for (1) budget bill provisions outlining the process for allocations from the HIPAA fund and (2) a proposed budget trailer bill permitting DHS to adopt unspecified emergency regulations to implement HIPAA.

Our analysis indicates that a statutory framework is warranted to guide a statewide project with the formidable size, scope, and complexity of HIPAA compliance. As we have noted earlier, many significant policy issues will arise from compliance efforts. Except for budgetary decisions, the administration's approach in effect largely excludes the Legislature from key policy decisions regarding the use of HIPAA funds and the governance, oversight, and administration of these activities.

RECOMMENDATIONS TO IMPROVE LEGISLATIVE OVERSIGHT OF HIPAA ACTIVITIES

We recommend that the Legislature approve the funding included in the budget to support state HIPAA compliance activities, but schedule all requested funds in the proposed new budget item (9909) for such activities. We further recommend the enactment of legislation to govern HIPAA compliance activities, limit the term of proposed HIPAA compliance positions, and replace the administration's proposed budget bill language with language that makes HIPAA allocations subject to state legislative requirements.

Fund All Activities Through HIPAA Fund. To adequately track all HIPAA allocations and expen-

ditures beginning in the budget year, we recommend that the Legislature delete all HIPAA proposals from the separate department budget items and instead schedule these allocations in the HIPAA fund budget item (9909). Allocations of reimbursements would be budgeted for the affected departments. The specific budget requests would be revised as follows:

- The DDS, $425,000 General Fund and $425,000 reimbursements.
- The DMH, $1.2 million General Fund and $1.2 million reimbursements.
- The DHS, $2 million General Fund, about $17 million reimbursements.
- The OSHPD, $79,600 federal funds.

Approve Positions for Two-Year Limited Terms. We also recommend that any positions requested by departments for HIPAA compliance activities be approved for two-year limited terms. Specifically, we recommend the following:

- The DMH, nine positions.
- The DHS, 15 positions.
- The OSHPD, one position.

Enact Legislation to Govern HIPAA Activities. We recommend the enactment of legislation to govern state HIPAA compliance activities that establishes a strong statutory framework appropriate for such a broad and complex statewide project. We recommend that the legislation include specific provisions that:

- Designate HHSA as the lead agency for state HIPAA compliance activities. We recommend HHSA for this role because the agency has the broad health policy and program expertise needed to direct and assist other departments in HIPAA compliance activities. Since non-HHSA departments will also be affected by HIPAA, the legislation should authorize HHSA to direct and monitor HIPAA compliance activities in those other departments.
- Direct HHSA to develop a statewide HIPAA compliance plan.
- Require departments to complete HIPAA assessments to determine the impact of HIPAA compliance on department operations.
- Establish appropriate time frames within which control agencies must complete reviews of departmental fund requests.
- Establish clear lines of authority over the administration of the HIPAA fund.
- Specify how funds will then be transferred and allocated from the HIPAA fund.
- Provide 30-day notification to the Legislature upon allocation from the HIPAA fund.

The legislation should be modeled on Chapter 608, Statutes of 2000 (AB 2817, Honda), which established oversight and other procedures for allocation of funding from the state's Information Technology Innovation Fund. Like Chap-

ter 608, the HIPAA legislation would establish criteria for project funding, assignment of responsibility for approving proposals, guidelines for funding requests, and procedures for notifying the Legislature regarding funding allocations.

Reject Proposed Budget Bill Language; Adopt New Budget Bill Language. We recommend that the Legislature reject proposed budget bill language for Item 9909-001-0001 relating to the allocation of the HIPAA fund. We recommend that the Legislature replace this language with budget bill language that ensures fund allocations are consistent with the proposed legislation. Specifically, we recommend the following budget bill language:

> Provision X. The funding provided in this item shall be available for expenditure contingent upon enactment of legislation in the 2001-02 legislative session specifying procedures for allocations from this item. Funding shall be expended consistent with any requirements of that legislation.

Acknowledgments

This report was prepared by Farra Bracht and Anna Brannen, under the supervision of Daniel C. Carson. The Legislative Analyst's Office (LAO) is a nonpartisan office which provides fiscal and policy information and advice to the Legislature.

❖

LAO Publications

To request publications call (916) 445-2375.

This report and others, as well as an E-mail subscription service, are available on the LAO's Internet site at www.lao.ca.gov. The LAO is located at 925 L Street, Suite 1000, Sacramento, CA 95814.