



County of Santa Cruz

HEALTH SERVICES AGENCY

P.O. BOX 962, 1080 EMELINE AVENUE
SANTA CRUZ, CA 95061
(831) 454-4066 FAX: (831) 454-4770

HEALTH SERVICES AGENCY
ADMINISTRATION

May 15, 2002

AGENDA: June 11, 2002

BOARD OF SUPERVISORS
County of Santa Cruz
701 Ocean Street
Santa Cruz, CA 95060

SUBJECT: Report on Health Insurance Portability and Accountability Act (HIPAA) Implementation

Dear Members of the Board:

Attached for your Board's review is a status report on the Health Services Agency's (HSA) implementation of the Health Insurance Portability and Accountability Act (HIPAA) passed by Congress in 1996.

In an effort to streamline administrative processes, protect the security of health care information systems and improve patient rights to privacy, this comprehensive law, when fully implemented, is expected to dramatically change many of the existing business and technology practices of the health care industry within the United States.

HSA has been monitoring HIPAA developments for some time and continues its ongoing planning efforts to comply with the law's provisions given the continued uncertainty and ongoing national debate over the law's implementation. Federal authorities are continuing to analyze the impact of HIPAA upon health activities and are making significant changes to the regulations implementing the legislation. HSA is working with the state and other health organizations to provide input and to understand the impact of the changes upon our operations.

In recognition of the implementation difficulties faced by health care organizations, the U.S. Department of Health and Human Services recently authorized a one-year extension to the law's data standards requirements for those health care entities that submit a compliance plan. HSA is recommending the County take advantage of this option to qualify for the extension.

It is, therefore, RECOMMENDED that your Board:

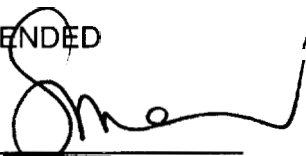
- 1) Authorize the Health Services Agency to submit the attached HIPAA compliance plan to the U.S. Department of Health and Human Services on behalf of the County of Santa Cruz; and
- 2) Accept and file this report.

Sincerely,



Rama Khalsa, Ph.D.
Health Services Administrator

RECOMMENDED



Susan A. Mauriello
County Administrative Officer

cc: County Administrative Office
County Counsel
Auditor-Controller
HSA Administration

Attachments:

Report: Implementation of the Health Insurance Portability and Accountability Act of 1996

Centers for Medicare & Medicaid Services - Electronic Health Care Transactions and Code Sets Standards Model Compliance Plan

REPORT TO THE COUNTY OF SANTA CRUZ BOARD OF SUPERVISORS:**IMPLEMENTATION OF THE HEALTH INSURANCE
PORTABILITY & ACCOUNTABILITY ACT OF 1996
(HIPAA)****Prepared by the Health Services Agency – May 2002****Background:**

In an effort to protect health insurance for American workers, streamline administrative processes in the health care industry and respond to growing public concerns about the need to protect individual rights of privacy, the U.S. Congress in 1996 adopted a comprehensive new law, the Health Insurance Portability and Accountability Act (HIPAA).

This law when fully implemented is expected to dramatically change existing business practices within the U.S. health care system.

HIPAA includes three main elements:

- **Administrative Streamlining:** Requires all health care providers, insurers and others involved with transmitting or receiving electronic health care information conform to nation-wide standards and coding systems when exchanging data electronically;
- **Data Security:** Requires health care organizations take specific steps to protect the security of health information they possess or exchange;
- **Patient Rights to Privacy:** Requires health care organizations to protect an individual's right to privacy regarding the sharing and dissemination of individually identifiable health information.

In August of 2000, the U.S. Department of Health and Human Services (DHHS), the agency charged with the responsibility of developing, administering, implementing and enforcing HIPAA regulations, issued its final regulations on Standards for Electronic Data Transactions (65 *FR* 50311). These regulations provide in great detail nation-wide data standards for electronic healthcare transactions including health claims, encounters, enrollment/dis-enrollment in a health plan, eligibility for services, healthcare payment, remittance advice, health plan premium payments, first report of injury, health claim status, referral certification and authorization.

This was followed in December of 2000 by the publication of regulations governing Privacy Standards for Individually Identifiable Health Information (65 *FR* 82461). These regulations have three major purposes:

- (1) To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information;
- (2) to improve the quality of health care in the U.S. by restoring trust in the system among consumers, health care professionals, organizations and individuals committed to the delivery of care; and
- (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection.

Final regulations are still being prepared for HIPAA security standards, various nation-wide employer, provider, health plan and patient identifiers, and other HIPAA requirements.

While the overall goals of HIPAA remain admirable and enjoy wide public support throughout the nation, detailed implementation of the law has become very complex and quite controversial in many quarters.

For example, recently the Bush Administration proposed changes to the existing HIPAA privacy regulations that would ease many of the requirements. Many elements of this proposed change are being fiercely battled in Congress and strong lobbying efforts are being mounted on both sides of this issue.

Implementation Deadlines:

While many of the elements of HIPAA implementation continue to be debated, currently, all covered health care entities within the U.S. including the County of Santa Cruz Health Services Agency (HSA) must meet the following deadlines for HIPAA implementation:

- **October 16th, 2002** - Implementation of HIPAA data standards must be completed for all health care organizations that have not submitted a HIPAA compliance plan extension.
- **April 14th, 2003** - Implementation of HIPAA privacy regulations must be completed.
- **October 16th, 2003** - Implementation of HIPAA data standards must be completed.

Due to ongoing issues regarding required data standards as discussed below, most HIPAA experts expect few if any health care organizations to be in compliance with the requirements by the original deadline of October of 2002. As a result, the U.S. Department of Health and Human Services (HHS) in March of this year issued procedures and forms for health organizations to submit HIPAA compliance plans and be granted an additional year to complete data standards compliance efforts.

Data Standards:

HIPAA imposes very specific data and coding standards for the transmission and reception of health information. These standards generally follow existing national standards organizations recommendations including: the American National Standards Institute (ANSI), the American Medical Association (AMA) American Dental Association (ADA), the U.S. Health Care Finance Administration (HCFA) and the Workgroup for

Electronic Data Interchange (WEDI). However, implementation of HIPAA data standards are requiring most health care organizations and institutions to revamp their computer software and in some cases computer hardware as well in order to comply.

In addition, some flaws and major omissions in the HIPAA data standards have been identified and solutions are currently being debated. There is a general recognition the standards are likely to be further modified prior to full-scale implementation.

In California for example, the State MediCal (Medicaid) system is highly dependent on what are known as "local codes" for electronic transactions. Similarly, mental and behavioral health systems at all levels rely on local or specialized code sets to conduct electronic transactions. Use of local and specialized codes will be prohibited under currently adopted HIPAA data standards.

Most experts are predicting data systems in the State of California and many systems nationally will not be HIPAA ready by the compliance deadlines.

Most of the electronic data transmissions HSA conducts are with State agencies. Even if HSA is in full compliance with HIPAA prior to the deadlines, it may not be able to conduct the electronic transactions as required under the law, because many of its business partners, including the State may not be compliant.

Many complexities remain to be resolved to achieve the administrative streamlining goals of HIPAA. Experts are predicting the resource and financial efforts necessary nation-wide to achieve compliance with HIPAA will far exceed the costs of Year 2000 compliance efforts. Costs have been estimated at \$20 to \$50 billion nationwide. The hope is that once data exchange has been standardized the ongoing costs related to health care administration will be dramatically reduced.

Privacy Standards:

Numerous public opinion polls demonstrate that medical records privacy for individuals is a major concern. Rights to medical privacy are widely supported by a large majority of Americans.

Fortunately, in California strong laws protecting patient privacy have been on the books for many years. Staff in HSA are well trained and mindful of the importance of protecting client privacy and confidentiality particularly as this relates to diseases that unfortunately continue to carry social stigma, such as mental illness, cancer, HIV/AIDs, sexually transmitted diseases, etc. Strong disciplinary sanctions exist for any violation of patient privacy or confidentiality requirements within HSA.

HIPAA requirements generally expand upon existing patient rights regarding medical record privacy. Generally, HIPAA prohibits the sharing of individually identifiable health information between parties except for the "minimum necessary" for medical treatment, payment and healthcare operations.

Initial HIPAA rules regarding medical privacy were adopted under the Clinton Administration in 2001. Recently, the Bush Administration has proposed modifications to the privacy rules that generally weaken privacy protections but also seek to eliminate

some of the more onerous requirements on medical providers that many argue if left unchanged would actually impede the ability to provide quality and timely medical care.

A national debate is currently underway in Congress in attempts to resolve these issues.

Security of Health Care information:

While DHHS has not yet issued final regulations governing the security of health care information, most HIPAA experts are recommending health care organizations begin their security planning efforts now. This should minimally include plans for:

- authentication of health care computer system users;
- computer system access controls
- monitoring of system access
- physical security and disaster recovery
- protection of remote access points and external electronic communications
- computer virus protection
- ongoing system security assessments
- organizational practices
- data encryption

HSA has always been vigilant in its computer security efforts and has already implemented many of the measures described above to protect the security of the health information it has responsibility for controlling. It is expected that HIPAA will require a more formalized approach to these security efforts once final security regulations are announced by DHHS.

HIPAA Resources:

HIPAA and its associated regulations currently consist of several thousand pages of documentation. Several new regulations are currently scheduled to be issued in coming months. Other HIPAA regulations continue to be prepared by the Federal Government.

HSA expects it will be several more years before all of the compliance issues regarding HIPAA implementation are fully completed.

In the meantime, there are a wide variety of resources available to health care organizations and the general public regarding HIPAA and its requirements. Much information is available on-line via the internet.

HSA continues to monitor HIPAA developments and changes in the law to help assure the County of Santa Cruz is well positioned to comply with all of the law's requirements. Some resources we would recommend for persons interested in finding out more information about HIPAA include:

<http://cms.hhs.gov/hipaa/> This is the official U.S. Government site regarding HIPAA.
<http://www.ohi.ca.gov/> The State of California Office of HIPAA Implementation
<http://www.chcf.org/> The California Health Care Foundation website
<http://www.hipaadvisory.com/> A HIPAA website sponsored by Phoenix Health Systems

Conclusions:

The Health Services Agency and its staff strongly support the overall goals of HIPAA as we believe administrative streamlining, data standardization, system security and patient privacy/confidentiality protections afforded by the law will ultimately improve the efficiency and quality of health care provided to the public.

As public health advocates, however, we would not be supportive of regulations that negatively impact on the ability of health care providers to best serve and attend to the health needs of their patients.

Efforts are currently underway at the national and state levels to find the appropriate balance between administrative efficiency, security, patient rights to privacy, and the myriad of other issues related to delivery of cost-effective quality health care in the 21st century. We are supportive of the ongoing public debate and are confident positive public health outcomes will be the result for our nation and for our community.

Sources:

U.S. Centers for Medicare and Medicaid Services

California Department of Health

Implementing the Federal Health Privacy Rule in California: A Guide for Health Care Providers, February, 2002 - Health Privacy Project - California Health Care Foundation

The Workgroup for Electronic Data Exchange

Centers for Medicare & Medicaid Services

Electronic Health Care Transactions and Code Sets Standards Model Compliance Plan

Section A: Covered Entity and Contact Information

1. Name of Covered Entity: County of Santa Cruz
 2. Tax Identification Number: 94-6000534
 3. Medicare Identification Number: W33339
 4. Type of covered entity:
 - Health Care Clearinghouse
 - Health Plan
 - Health Care Provider - Other
 5. Authorized Person: Dr. Rama Khalsa
 6. Title: Health Services Agency Administrator
 7. Street: 1080 Emeline Ave.
 7. City/State/ZIP: Santa **Cruz**, CA 95060
 8. Telephone Number: (831) **454** - 4000
-

Section **B**: Reason for Filing for This Extension

10. Please check the box next to the reason(s) that you do not expect to be compliant with the HIPAA Electronic Health Care Transactions and Code Sets standards (45 C.F.R. Parts 160, 162) by October 16, 2002. Multiple boxes may be checked.

- Need more money
- Need more staff
- Need to buy hardware
- Need more information about the standards
- Waiting for vendor(s) to provide software
- Need more time to complete implementation
- Need more time for testing
- Problems implementing new clinical code sets

DRAFT

**Problems completing additional data requirements
Need additional clarification on standards**

Section C: Implementation Budget

This question relates to the general financial impact of the HIPAA Electronic Health Care Transactions and Code Sets standards (**45 C.F.R. Parts 160,162**) on your organization

11. Select from the drop-down menu the range of your estimated cost of compliance with the HIPAA Electronic Health Care Transaction and Code Sets standards (**45 C.F.R.,Parts 160,162**):

\$500,000 - \$1 Million

Section D: Work Plan/Implementation Strategy/Testing Schedule

This section encompasses HIPAA Awareness, Operational Assessment, Development and Testing, all of which are collectively referred to as the Transactions and Code Sets Implementation Process. For more details on completing each of these subsections, refer to the "Help on this question" links for each individual question.

Phase One - HIPAA Awareness

These questions relate to your general understanding of the HIPAA Electronic Health Care Transactions and Code Sets standards (**45 C.F.R. Parts 160,162**).

12. Please indicate whether you have completed this Awareness phase of the Implementation Process.

No

13. Projected/Actual Start Date: **September, 2001**

14. Projected/Actual Completion Date: **January, 2003**

Phase Two - Operational Assessment

These questions relate to HIPAA operational issues and your progress in this area.

15. Please indicate whether you have completed this Operational Assessment phase of the Implementation Process.

No

16. Reviewed current processes against HIPAA Electronic Health Care Transactions and Code Sets(45 C.F.R Parts 160,162)requirements?

Initiated But Not Completed

17. Identified internal implementation issues and developed workplan?

Initiated But Not Completed

18. Decided whether to use the services of a vendor or other contractor?

Yes

19. Projected/Actual Start Date: **August, 2001**

20. ProjectedActual Completion Date: **March, 2003**

Phase Three - Development and Testing

These questions relate to HIPAA development and testing issues. ASCA legislation requires that testing begin no later than April 16,2003. For more details, refer to the "Help on this question" links for each individual question.

21. Please indicate whether you have completed this Development and Testing phase of the implementation process.

No

22. Completed software development/installation?

Initiated But Not Completed

23. Completed staff training?

Initiated But Not Completed

24. ProjectedActual Development Start Date: **September, 2001**

25. ProjectedActual Initial Internal Software Testing Start Date: **April, 2003**

26. Projected/Actual Testing Completion Date: **August, 2003**
