



Can You Meet The HIPAA Requirements?

The 2nd National HIPAA Summit

March 2th, 2001

Dorothy M. Webman, D.S.W.
President, Webman Associates
Chair, The Work Group for the
Computerization of Behavioral Health
and Human Services Records

Jean Campbell PhD.
Research Assistant Professor
Missouri Institute of Mental Health

Dr. Ronald Manderscheid
Chief Survey and Analysis
Center for Mental Health Services
Substance Abuse and Mental Health
Services Administration
U.S. Department of Health and
Human Services



What is HIPAA and What is Administrative Simplification?

The Health Insurance Portability and Accountability Act of 1996

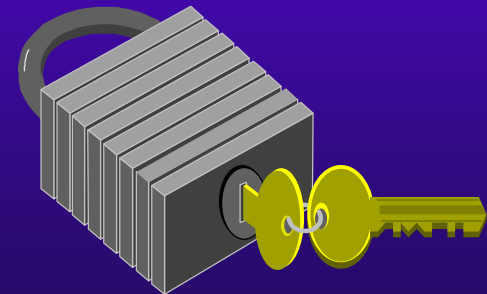
Signed August 21, 1996 to become P.L. 104-191

Administrative Simplification Subtitle
Added Part C of Title XI to the Social Security Act



Purpose of Provisions

- ◆ Improve the efficiency and effectiveness of the health care system by standardizing the electronic data interchange of certain administrative and financial transactions.
- ◆ Protect the security and privacy of transmitted information.





What are the HIPAA Administrative Simplification Requirements?

- ◆ 9 specific EDI transaction standards (claims, enrollment, etc.) including code sets.
- ◆ Coordination of benefits information.
- ◆ Unique identifiers (including allowed uses) for individuals, employers, health plans, and health care providers.
- ◆ Security, confidentiality, and electronic signatures.
- ◆ Privacy for Individually Identifiable Health Information
- ◆ Others adopted by HHS, possibly including the EMR



What is a Covered Entity?

◆ Covered Entities

- Health care **providers** who transmit health information electronically in connection with standard transactions
- All health **plans**
- All health care **clearinghouses**

◆ Authority not comprehensive

- Regs **do not** apply directly to other entities such as:
 - agents or contractors of covered entities,
 - employers, life insurers, and researchers.



What is the time table???

- ◆ **October 2002** is the effective date for most of the **Transaction Codes** (claims, payment, enrollment, eligibility, premium payment, referral fpr pharma, (except patient information and report of first injury which will be effective in 2003)
 - Processed 17,000 comments
- ◆ **February 2003** is the expected effective date for the **Privacy Rule**
 - processed 150,000 comments
- ◆ The comment period has closed for the national provider Id, employer ID, and Security rule – effective dates are not yet available.



What is the Cost Equation?

- ◆ The government estimates :
 - total savings from the EDI standards will be 29 billion.
 - these savings will be offset by the cost of privacy implementation which is estimated at 17.6 billion.
 - there will be a net savings of 12.6 billion over ten years
- ◆ However, private research firms and others implementing the rules have noted that government cost and savings estimates are highly inaccurate.
- ◆ Most estimate that costs will be 2-10 times that of Y2K spending.
- ◆ In the health care arena alone this could entail as much as 80 billion in cost!



What are the penalties?

- ◆ Civil Penalties of \$100 per incident, up to \$25,000 per person, per year, per standard violated.
- ◆ Federal Criminal Penalties, up to \$250,000 and up to 10 years in prison for knowingly and improperly disclosing or obtaining protected health information
- ◆ **NOT GETTING PAID!!!** If you do not submit claims in a manner consistent with the new standards you will not get paid!



What is the Value Proposition?

- ✓ Gaining a competitive edge in the information economy by building consumer trust
- ✓ Reducing operating costs by eliminating the collection and management of unnecessary information.
- ✓ Reducing risks associated with the use of inaccurate or out-of-date information.
- ✓ Increase public image as a leader in privacy
- ✓ Reducing risks associated with failure to comply
- ✓ Improving relationships with employees who can trust their employer to handle their personal information securely.



Who Is Representing Behavioral Health In The HIPAA Dialogue?

- ◆ SAMHSA
- ◆ The Work Group
- ◆ MHSIP
- ◆ NASMHPD
- ◆ National Associations such as APA, NASW, AMBHA
- ◆ National Advocacy Groups: Federation of Families for Children's Mental Health, NAMI, Bazelon, NMHA



Work Group Mission

- ◆ To create and promote equitable standards for information access, privacy and confidentiality, including informed consent.
- ◆ To create, monitor, and promote standards or guidelines for assessing the quality of behavioral health and human services records.
- ◆ To promote sharing of data, consumer education and to develop a collaborative protocol for stakeholder participation.



How Does HIPAA Impact Behavioral Health?

- Starting in second place with a lack of funds
- Data Sets: DS 2000+ and other HHS standards
 - currently being addressed by the MSHIP and the Workgroup
- Procedure Codes: major gap
 - currently being addressed by NASMPHD
- Privacy: the Workgroup has determined that there is a lack of consensus on these matters
- IRB's and Privacy Boards: need special training
- More stringent local and federal regulations, such as the Substance Abuse confidentiality regulations and local special population exemptions, also need to be mediated.
- Security: seriously lack of attention to security !
- Training, education and outreach
 - **Work Group, MHSIP and nationals are trying!**



The Work Group's Take: **Allied Health & HIPAA**

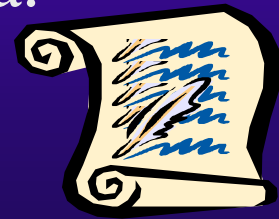
- ◆ Allied health organizations include the Departments of Health and Human Services, Education, and Justice.
- ◆ Allied health organizations are not aware of HIPAA but are bound by its mandates.
- ◆ Please allow us to develop and submit for your review a list of the types of services and activities allied health organizations engage in that make them appear to be a covered entity under HIPAA.





More Allied Health & HIPAA

- ◆ Please study the burden on allied health organizations to reach HIPAA compliance
- ◆ Ensure availability of outreach, training and technical assistance required to bring these agencies and entities into HIPAA, HCFA security standards and privacy rule compliance.
- ◆ Explore the viability of engaging allied health organizations and agencies in the process of streamlining their administrative data.





Federal Substance Abuse Confidentiality Requirements.

- ◆ The federal confidentiality of substance abuse patient records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR Part 2, establish confidentiality requirements for patient records that are maintained in connection with the performance of any federally-assisted specialized alcohol or drug abuse program.
- ◆ The term "federally-assisted" is broadly defined and includes federally conducted or funded programs, federally licensed or certified programs, and programs that are tax exempt. Certain exceptions apply to information held by the Veterans Administration and the Armed Forces.



Disclosures are Permissive, and NOT Mandatory

- ◆ There are a number of health care providers that are subject to both these rules and the substance abuse statute and regulations.
- ◆ In most cases, a conflict will not exist between these rules.
- ◆ These privacy rules permit a health care provider to disclose information in a number of situations that are not permitted under the substance abuse regulation.
 - I.e., disclosures allowed, without patient authorization, under the privacy rule for law enforcement, judicial & administrative proceedings, public health, health oversight, directory assistance, & as required by other laws would generally be prohibited under the substance abuse statute & regulation.
- ◆ Because these disclosures are permissive and not mandatory an entity would not be in violation of the privacy rules for failing to make these disclosures.



Informed Consent in Substance Abuse Settings

- ◆ The substance abuse regulation requires notice to patients of the substance abuse confidentiality requirements and provides for written consent for disclosure.
- ◆ While the privacy rules have requirements that are somewhat different, **the program may use notice and authorization forms that include all the elements required by both regulations.**
- ◆ The substance abuse rule provides a sample notice and a sample authorization form and states that the use of these forms would be sufficient.
- ◆ While these forms DO NOT satisfy all of the requirements of the privacy regulation, there is no conflict because the substance abuse regulation does not mandate the use of these forms.



What Can You Do?

- ◆ Get compliant!
- ◆ Educate your legislators about the need for more funds in behavioral health budgets to address Administrative Simplification Requirements
- ◆ Educate everyone you know about the unique privacy concerns of persons with disabilities and persons with behavioral health problems.
- ◆ Join the Behavioral health task forces (work group, mhsip, roundtables etc) and get active with your advocacy and professional associations.
- ◆ Get plugged into the local and national Data Standards, Privacy and Security action networks



What's This All About?

– “*Everything on the Web is ultimately about Trust*”

– -- Nicholas Negroponte



Consumer Fears

- ✓ Protection of home and family
- ✓ Disclosure of medical, genetic data
- ✓ Discrimination, redlining and other bigotry
- ✓ Disclosure of indiscretions, private lives, other personal secrets



*“Privacy is
like oxygen.
We really
appreciate it
only when it
is gone.”*

Charles J.
Sykes, “The
End of
Privacy”

Consumer Wishes

- ◆ Convenience
- ◆ Speed
- ◆ Personalization or Anonymity (at times)
- ◆ Control
- ◆ Explicit and clear privacy T/C
- ◆ Various trust and information assurance mechanisms
- ◆ Data differentiation



As Little As Possible...

...As Much As Necessary

- ◆ Nothing About Us Without Us!
- ◆ Informed Consent
- ◆ Desire for Improved Care Coordination
- ◆ Consumer Outreach and Training
- ◆ Consumer Ownership and Control of Personal Information
- ◆ Consumer Driven System



Coming to Terms

- ◆ **Privacy** is the *right* of the individual to be left alone
- ◆ **Confidentiality** is the *responsibility* for limiting disclosure of private matters
- ◆ **Security** is the *means* to control access and protect information from accidental or intentional disclosure



Basic Privacy Lexicon

◆ Fair Information Practice Principles:

- Notice/Awareness – Customers must be given notice before information is collected
- Choice/Consent – Customers must have options on whether and how information is collected and used
- Security/Integrity – Reasonable steps must be taken to assurance correctness and security
- Enforcement/Redress – Compliance mechanisms and sanctions for violators



Regulation Leading the Way...

- ◆ HIPAA
 - Administrative Simplification
 - Privacy Regulation
- ◆ FERPA (Family Educational Right and Privacy Act)
- ◆ COPPA (Children's Online Privacy Protection Act)
- ◆ GLB (Gramm Leach Bliley Act)
- ◆ HCFA Internet Security Standards
- ◆ FTC Financial Data Transaction Standards
- ◆ CALINX
- ◆ Europe-wide Privacy Standards





Beyond HIPAA/GLBA_(just a sample)

- ◆ Medical Financial Privacy Bill (H.R. 4585) -- Among other things, the bill requires a specific and separate consent for mental health information, HIV information, genetic information, and abortion information.
- ◆ Competitive Market Supervision Act (S. 2107):
 - Amendment 21 would restrict the sharing of Social Security Numbers (designed to address identity theft and stalking, but could hamper legitimate business activities)
 - Amendment 22 provides special protections of PII to consumers with a disability as defined in the ADA
 - Amendment 23 would require that financial institutions specifically disclose policies and practices of sharing of individually identifiable health information to affiliates and non affiliated third parties.




The Work Group's Responses to DHHS

- ◆ We were proud to be included in some phases of this process. Yet we are concerned that the voice of behavioral health and human services has not yet been incorporated ... consumer groups have not been as actively involved in the process as they could be.
- ◆ Please develop, with the guidance of experienced persons, more detailed privacy regulations and data sets that are specific to behavioral health and human services aspects of integrated health care systems.

Excerpts of Comments on Consumer Concerns

- ◆ We urge you to move consumer concerns to the forefront of your agenda by incorporating mechanisms for consumers to read, write on, and access their records at any moment in time.
- ◆ We also respectfully request that you include more far-reaching recommendations for consumer education about their privacy rights.
- ◆ Furthermore, we implore you to mandate informed consent standards for every transaction of individually identifiable information.



*“Nothing
about us
without
us!”*



*“Meet
the
client
where
the
client is
at...”*

Excerpts of Field Comments on Clinical Considerations

- ◆ **Advanced Directives:** There should be provisions for Advanced Directives, so the individual can designate those who have access to his health care records. These provisions should protect the health care records of the individual from unauthorized access.
- ◆ **Psychotherapy Notes:**
 - It’s the nature of data not the format in which it is requested ...
 - This exemption should cover all sensitive information about ‘special populations’
 - APA, NASW, NASMHPD, NAMI, FEDERATION, all concur with Work Group on matter of psychotherapy notes
 - and AMBHA agreed but with a caveat about the information that should be in a medical record and not covered under the psychotherapy note exemption.



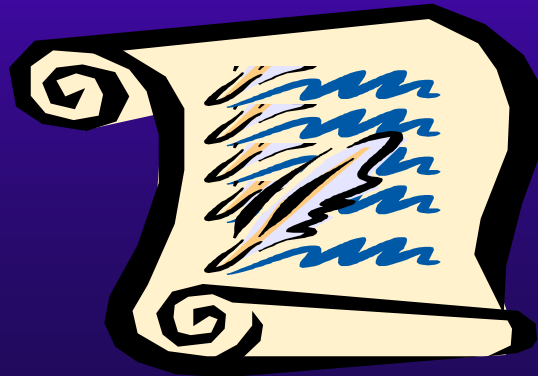
Pre-emption: Field Response

- ◆ APA, NASW, NASMHPD, NAMI, FEDERATION, all concur with Work Group that the pre-emption clause which allows more stringent local laws and regulations override HIPAA is a good one.
- ◆ Most also seemed to be of the mind set that states should not be granted waivers to allow the continued use of less restrictive policies. A few state agencies commented that this provision should better account for timeliness of DHHS responses to waivers and allow continued use of less stringent regulation until waiver review is complete.
- ◆ Many advocates call for one federal guideline.



Minimum Necessary: Field Response

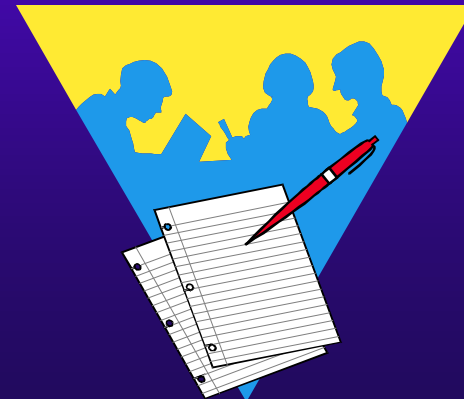
- ◆ APA, NASW, NASMHPD, NAMI, FEDERATION, AMBHA all concur with Work Group that the secretary was wise to invoke a minimum necessary guideline.
- ◆ However, the Work Group also believes that providers still retain too much control over these decisions and would have preferred language that left minimum necessary decisions to the joint discretion of providers and consumers.



Informed Consent ala Work Group

- ◆ Leave blanket consent.
 - Standard Form – quality and format of form
 - Insert form item: resale of information
 - Please create special provisions for disclosure of sensitive information
- ◆ Please consider future use of new technologies to enable informed consent for EVERY disclosure.

"There were more than 30,000 comments from consumers ... most wanting control over every disclosure of their health information!"





Data Privacy and Security

“Not content with snatching her body, Starr’s deputies were now invading her mind. They had exposed her sex life and dissected her personality; now they wanted to scrutinize her very soul. It was an invasion too far.”

Monica’s Story, Andrew Morton



Planning for Privacy and Security

- ◆ Yes, you do need a plan
- ◆ No, there isn't a single solution
- ◆ Why a framework is essential
 - It defines a set of parameters in which privacy policies, procedures, practices, and technology can be implemented, supported and audited.



Who Clears On the Policy?

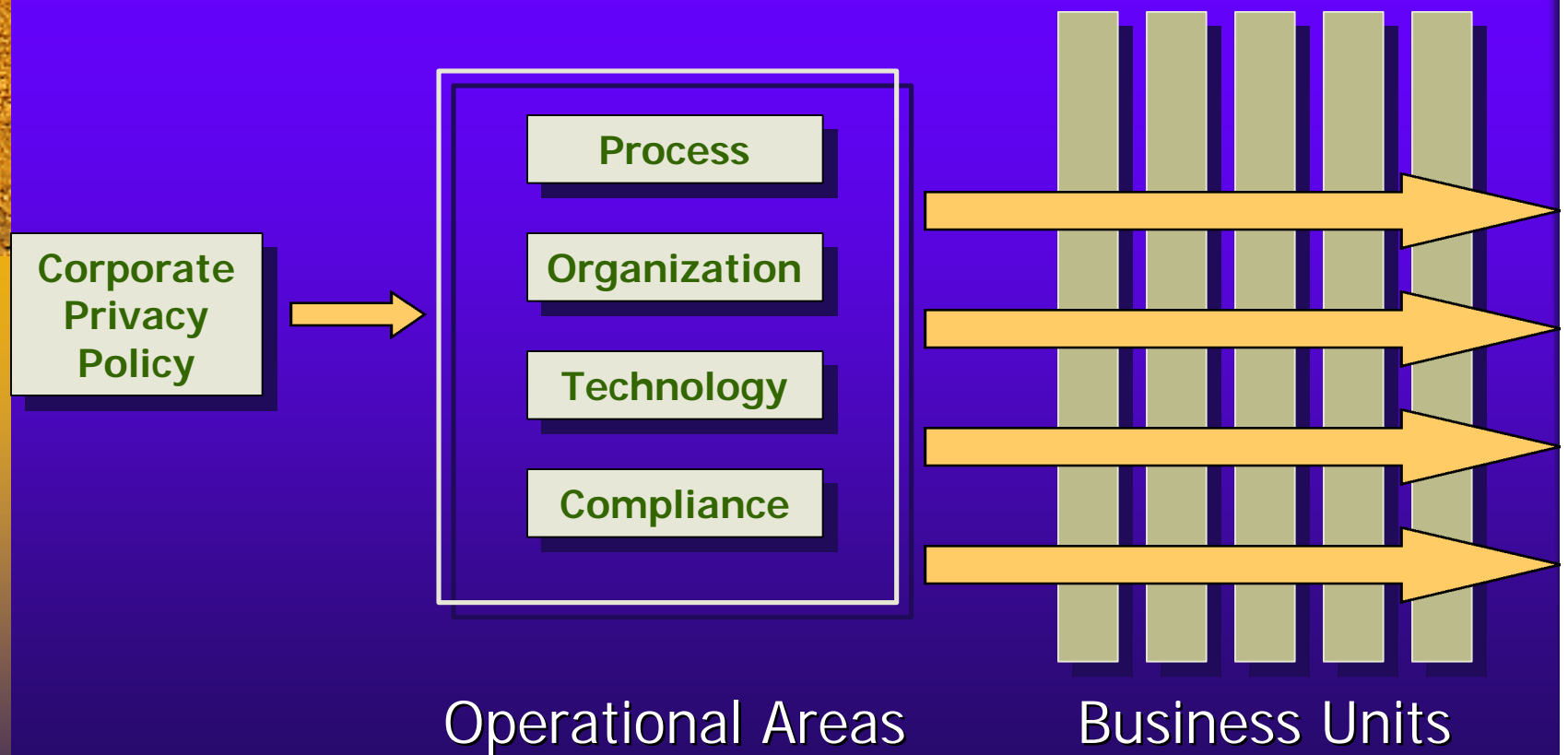
- ◆ Short Answer: Everyone
- ◆ Better Answer:
 - CEO
 - Task Force
 - Consumers
 - Business Units (Products and Operations)
 - General Counsel
 - Government Affairs
 - Information Security
 - I/T



Work Plan

- ◆ Understanding your new policy and the current gaps, develop a compliance strategy and an project plan that will mitigate these risk areas:
 - Organization
 - Process
 - Technology
 - Compliance

Assess Privacy Policy Impact





Online Privacy Notices

Should reflect online privacy best practices- must be accurate for the institution

Must meet applicable regulatory requirements

Must be consistent across e-business presence and with offline statements





Privacy Failure Consequences

- Irreparable damage to reputation, consumer retention, trust and customer-focused business strategy
- Loss of revenue and new business
- Interruption of transborder data flows, applicable penalties in international jurisdictions
- Possible federal, state enforcement actions- millions of dollars spent and loss of flexibility in marketplace to implement consent decrees, irreparable damage to key business initiatives such as eBusiness
- Litigation from consumers, privacy advocates, business partners
- Civil and criminal penalties for wrongful disclosure of protected health information



Security Bottom Line

- ◆ The information in statutes and proposed rule is somewhat vague -- basically, you have to have a real security program in place
- ◆ You need to meet a demonstrable “standard of due care”
- ◆ If you don’t already have support for your security program, add this fuel to the fire



Framework Building Blocks - Architecture and Technology

- ◆ Policies and procedures build the foundation for technology use practices
- ◆ The technology does the end work of encrypting, storing, and transporting the data
- ◆ Don't forget the legacy, be realistic about constraints
- ◆ Incorporate the privacy technology, don't bolt it on



Framework Building Blocks - Tools in the Toolbox

- ◆ Perimeter
 - Firewalls, Intrusion Detection
- ◆ Identification, Authentication, Authorization
 - Two-factor, data segmentation, directory services, role-based access
- ◆ PKI/Encryption
 - Digital Ids, Digital signatures, VPNs, S/MIME
- ◆ Access Auditing
 - Notice, data integrity, Opt In/Opt Out



3rd Party Certification

- ◆ Consider the value of 3rd party assurance services/seals
- ◆ Third party assurance will become the norm especially for B2B relationships





Designated Standard Maintenance Organizations

DSMOs are those organizations that agree to maintain the standards adopted by the Secretary.

These DSMOs have formed a committee to focus on managing HIPAA standard change requests. This web site www.hipaa-dsmo.org helps meet that challenge by providing industry expertise and solutions that directly support several of the committee's guiding principles:

- Allow open public access
 - Provide for timely review
 - Cooperate and communicate
 - Consider all viewpoints
- You can [search](#) for and view requested changes, but must [register](#) and log in to request a change. Consider checking the [Frequently Asked Questions](#) before requesting a change.

The X12N Transaction Standards, as well as the HL7 Attachment Standards are available on the [Washington Publishing Company](#) web site. Information about the NCPDP Retail Pharmacy Standards are available on the [NCPDP](#) web site.



Designated Standard Maintenance Organizations - continued

Pursuant to §162.910, the Secretary designates the following organizations as DSMOs:

Accredited Standards Committee X12

www.x12.org

- Dental Content Committee of the American Dental Association
www.ada.org
- Health Level Seven
www.hl7.org
- National Council for Prescription Drug Programs
www.ncpdp.org
- National Uniform Billing Committee
www.nubc.org
- National Uniform Claim Committee
www.nucc.org

Decision Support 2000+

- ◆ Population Data
- ◆ Enrollment Data
- ◆ Encounter Data
- ◆ Cost Data
- ◆ Clinical Guidelines
- ◆ System Guidelines
- ◆ Consumer Outcomes
- ◆ System Performance - Report Cards
- ◆ Human Resources Data





Information Systems Drive It All

- ◆ The Mandates of HIPAA's Administrative Simplification Act & CALINX
- ◆ The Cornerstone of Managed Care
- ◆ Decision Support 2000+
 - Intercare Project - Europe
- ◆ Web-Based Solutions:
 - The Virtual, Consumer-Driven Health, Behavioral Health
and Human Services Information System
- ◆ Government Computerized Patient Record (GCPR.gov)



HIPAA, Administrative Simplification and Technology

- ◆ HIPAA puts the wind in EDI
- ◆ Enables legal use of the Net
- ◆ Presents an opportunity to update legacy systems

HOWEVER . . .

Beware of HIPAA Vaporware!



Ideal Characteristics of the System

- ◆ Security
- ◆ Availability – consumer driven
- ◆ Affordability
- ◆ Productivity
- ◆ Multidimensionality
- ◆ Integration





Ideal Characteristics of the System (*continued*)

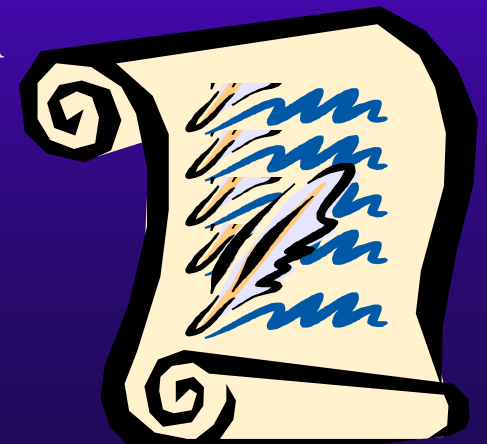
- ◆ Correction
- ◆ Outcome-oriented
- ◆ Sensitivity
- ◆ Platform independence





The Work Group's Take: Allied Health & HIPAA

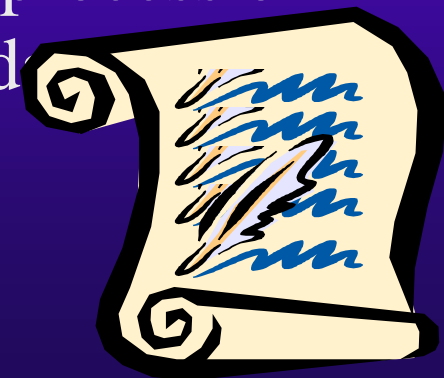
- ◆ Allied health organizations include the Departments of Health and Human Services, Education, and Justice.
- ◆ Allied health organizations are not aware of HIPAA but are bound by its mandates.
- ◆ Please allow us to develop and submit for your review a list of the types of services and activities allied health organizations engage in that make them appear to be a covered entity under HIPAA.



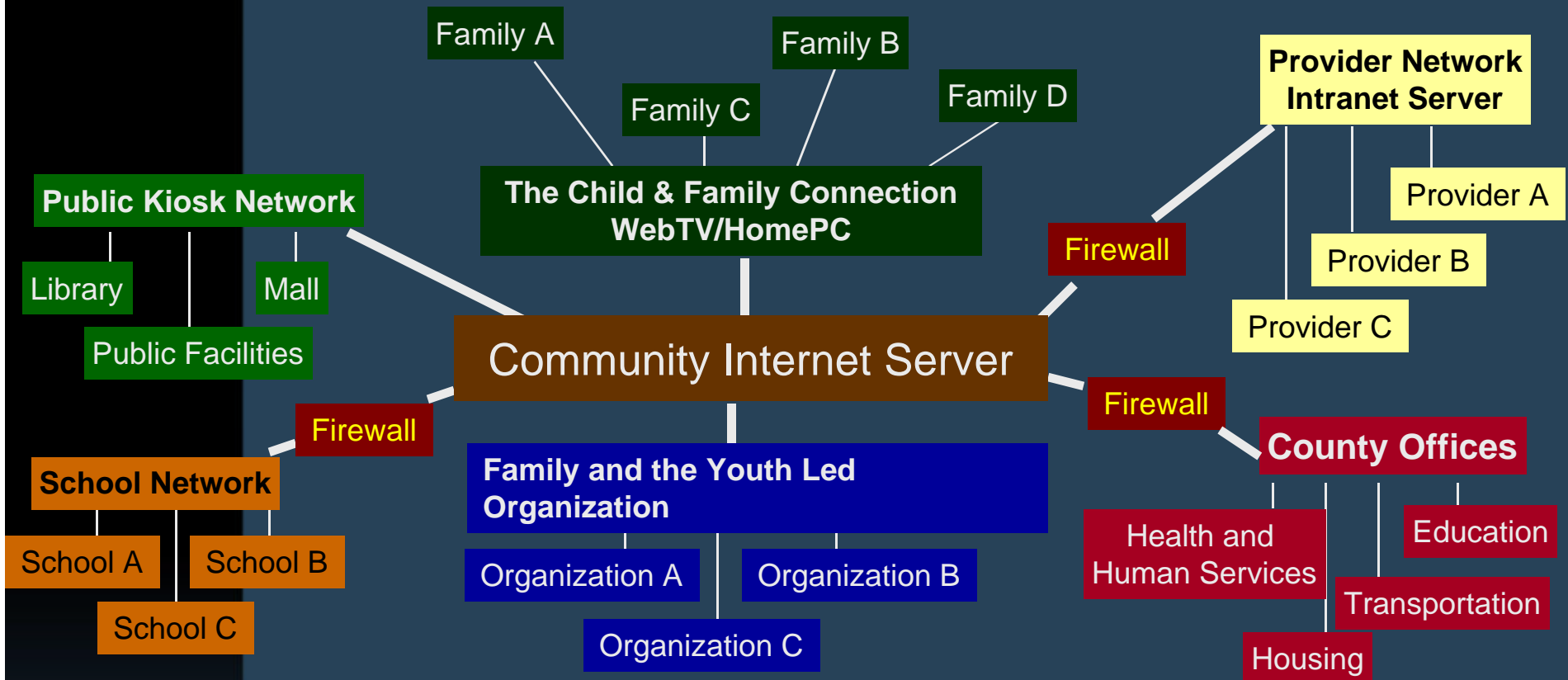


More Allied Health & HIPAA

- ◆ Please study the burden on allied health organizations to reach HIPAA compliance
- ◆ Ensure availability of outreach, training and technical assistance required to bring these agencies and entities into HIPAA, HCFA security standards and privacy rule compliance.
- ◆ Explore the viability of engaging allied health organizations and agencies in the process of streamlining their administrative d



The Electronic Community



Functions on Server

| | |
|-----------------------------|---------------------|
| E-mail | • Provider Profiles |
| Resource Directory | • Report Cards |
| • Eligibility Determination | • Family & Consumer |
| • Assessment & Referral | • Satisfaction |
| School/Job Search | |

Health and Human Services

| | |
|--|---------------------|
| • Juvenile Justice | • Child Welfare |
| • Public Health | • Special Education |
| • Child Mental Health | • Medicaid |
| • Children's Health Insurance Program | |
| • Substance Abuse Prevention & Treatment | |
| • Temporary Assistance to Needy Families | |



Challenges

- ◆ Protecting privacy
- ◆ Ensuring trust
- ◆ Working with legacy systems
- ◆ Implementing HIPAA, DS2000+, AFCARS....
- ◆ Interagency data collection & sharing
- ◆ Developing real time data analysis capacity
- ◆ Transferring sensitive information to & from public information highways
- ◆ Developing secure information infrastructures to advance service effectiveness and research



Successful Implementation =

- ◆ Business Process Analysis +
- ◆ Business Process Redesign +
- ◆ Change Management +
- ◆ Technology to Support It All!



Nurturing Change



Peer Consultation



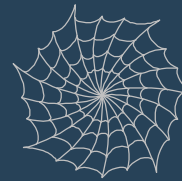
Exposure to web technology for outcome measurement



Exposure to web-based data transfer of self help



Exposure to web-based data transfer of family advocacy data



Exposure to web-based data transfer of referral data



Influence the development of state of the art technologies in children's systems of care



Ability to:

Improve quality of care



Outcomes for children and families



Practical Next Steps

- ◆ Get consumers involved today!
- ◆ Appoint or Outsource a HIPAA team, Privacy Officer and Security Officer today
- ◆ Establish relationships with Privacy Boards
- ◆ Conduct necessary assessments, risk analyses, and gap analyses
 - Assess current & desired business process models
 - Evaluate data content and transaction procedures
- ◆ Develop Compliance and Value-Driven HIPAA Strategy
 - Develop business process re-engineering, technology and change management plans
 - Create and implement data privacy and security plan
- ◆ Develop comprehensive training & outreach plan
- ◆ Interact with DSMO's
- ◆ Right size your plan of action!



Get HIP & GET IT!

- ◆ Get a Team
- ◆ Get Data Savvy, Privacy Protected, Security Assured
- ◆ Get Legal Counsel
- ◆ Get Involved
- ◆ Get Compliant
- ◆ Get Real (time)
- ◆ Get Value
- ◆ Get HIP – Aaaaaaaa!



Non-profits & Government Entities in the Behavioral Health Space

- ◆ workgroup.org
- ◆ samhsa.gov
- ◆ mhsip.org
- ◆ ffcmh.org
- ◆ gcpr.gov
- ◆ mentalhealth.org/specials/surgeongeneralreport
- ◆ Public Health Data Consortium -
<http://www.cdc.gov/nchs/otheract/phdsc/phdsc.htm>
- ◆ Office of Civil Rights -
<http://www.hhs.gov/ocr/hipaa.html>



Sample Tool Kits

- ◆ Ncpdp.org – transaction standards and data set compliance kit
- ◆ Wpc-edi.com EDI implementation guides
- ◆ Guidelines for Effective Privacy Policies
<http://www.privacyalliance.org/resources/ppguidelines.shtml>
- ◆ Guidelines for Effective Enforcement of Self-Regulation
<http://www.privacyalliance.org/resources/enforcement.shtml>
- ◆ Principles for Children's Online Activities
<http://www.privacyalliance.org/kidsprivacy/>
- ◆ Call For Action's "ABC's of Online Privacy"
<http://www.callforaction.org/abc.html>
- ◆ Patient-Centered E-Mail Guidelines
<http://www.mahealthdata.org/mhdc/mhdc2.nsf/e214ac63ff65c87e852564580073a9fd/4a7c6d398962159785256759006a1113?OpenDocument>
- ◆ Privacy Survival Guide
<http://www.privacyrights.org/fs/fs1-surv.htm>



A Few of Many Privacy Links

Regulatory

- ◆ GLB: <http://www.bog.frb.fed.us/BoardDocs/Press/BoardActs/2000/20000621>
- ◆ FTC: <http://www.ftc.gov/acoas/papers/finalreport.htm>
- ◆ HIPAA: <http://aspe.hhs.gov/admsimp/>
- ◆ EU: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html
- ◆ HCFA: <http://www.hcfa.gov/security/iseclpcy.htm>

General Info

- ◆ <http://www.privacyexchange.org>
- ◆ <http://www.epic.org>
- ◆ <http://www.privacyplace.com>
- ◆ <http://www.eff.org>
- ◆ <http://www.leglnet.com/libr-priv.htm>
- ◆ <http://www.privacyalliance.org>
- ◆ <http://www.healthcaresecurity.org>



Some Good Books

- ◆ “The Transparent Society”, David Brin, ISBN 020132802X
- ◆ “The Unwanted Gaze”, Jeffrey Rosen, ISBN 0679445463
- ◆ “The Hundredth Window : Protecting Your Privacy and Security in the Age of the Internet”, Charles Jennings, Lori Fena, ISBN 068483944X
- ◆ “For the Record : Protecting Electronic Health Information”, Computer Science and Telecommunications Board, ISBN 0309056977
- ◆ “1984”, George Orwell, ISBN 0451524934
- ◆ “Brave New World”, Aldous Huxley, ISBN 0060929871



Questions?

dwebman@webmanassociates.com

rmanders@samhsa.gov

campbelj@mimh.edu

& please visit our new website:

www.workgroup.org