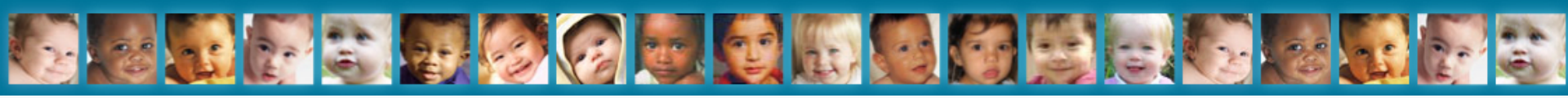
Introducing Valerie Watzlaf, PhD

- Dept. of Health Information Management, School of Health and Rehabilitation Sciences, University of Pittsburgh
- American Health Information Management Association (AHIMA)
- Researching the development of standards for the content of the EHR/VoIP, automated coding and anti-fraud systems, and the impact of ICD-10-CM on public health reporting.

NCHAM
National Center for Hearing Assessment and Management
Utah State University™



Privacy and Security Assessment for Internet-based Technologies (VoIP)

Valerie Watzlaf, PhD, RHIA, FAHIMA
Sohrab Moeini, MS
Laura Matusow, BS, RHIA
Patti Firouzan, MSIS, RHIA
University of Pittsburgh
School of Health and Rehabilitation Sciences
Department of Health Information Management

Outline

- Introduction
  - Telerehabilitation
  - Voice over Internet Protocol (VoIP)
  - HIPAA
    - New amendments – American Recovery and Reinvestment Act (ARRA) and Health Information Technology for Economic and Clinical Health (HITECH)
- Privacy/Security Checklist
- Risk Assessment of current VoIP landscape
- Recommendations
- VISYTER

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

Telerehabilitation

- (ATA—TR SIG) Blueprint TR Guidelines
- Assessment, monitoring, prevention, intervention, supervision, education, consultation, counseling
- Telespeech, teletherapy, telepractice

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

Telerehabilitation

- Privacy and confidentiality of telerehab technology
- Client awareness of rights and responsibilities
- Equipment, regulations, protection of client information, training, strategies environmental care, infection control, ethics

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

Voice over Internet Protocol (VoIP)

- Voice and Video teleconferencing
- Important service for rural clients
- Low cost
- Eliminates travel time and office wait times
- Some users believe they are HIPAA compliant

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

Voice over Internet Protocol (VoIP)

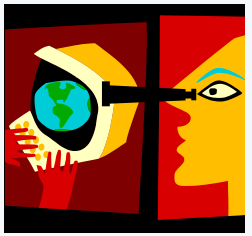
- Need to comply with the new HIPAA provisions VoIP is considered a business associate

- Important for entities that use VoIP systems to address and comply with the privacy and security guidelines and HIPAA requirements.

- Perform a Risk Analysis on the Privacy and Security of VoIP systems

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

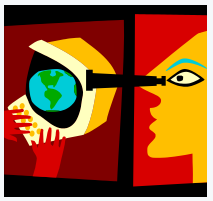
ARRA/HITECH—HIPAA



- Uncertainty exists between healthcare providers, information technology experts, etc. as to whether VoIP is private, secure, and HIPAA compliant.
- Confusion over whether VoIP systems like Skype, ooVoo etc. are considered BAs and therefore must meet the new HIPAA requirements

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

ARRA/HITECH--HIPAA



- Per DHHS, “Any entity that works on behalf of a covered entity is generally a business associate if they handle PHI.” www.hhs.gov/ocr/privacy
- If VoIP is a BA, then under the new rules they are subject to certain provisions of the HIPAA amendments, such as reporting security breaches to the CEs in 60 days after discovery as well as the civil and criminal penalties for violations.

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

VoIP Privacy and Security Checklist: Privacy

- **Personal Information**
  - Listening in
  - Accessible to Employees of VoIP
  - Sharing of content to protect legal interests
  - Shared with 3rd party
  - Time to comply with changes to privacy policy
  - Amending PHI
  - User contact's see online
- **Retention of Personal Information**
  - Recorded and stored
  - Length of time retained
  - Client delete information
  - Level of access up to user
  - User archive on network devices

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

VoIP Privacy and Security Checklist: Privacy

- **Requests from Legal Authorities etc.**
  - Communication content shared with LA
  - Will user know of disclosure
  - Background of employees providing this information
  - Appropriate processing of request
  - Accounting of disclosures
  - Client restriction of uses and disclosures
- **Sharing of Personal information in Other Countries**
- **Linkage to Other Websites**
  - With other privacy policies
  - VoIP accept responsibility for these other sites
  - Other sites comply with privacy and security requirements (HIPAA)
- **Voicemail**

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

VoIP Privacy and Security Checklist: Security

- Encryption
  - Strong encryption algorithms during transmission
  - Protect eavesdropping
  - Include what encryption entails
- Anti-Spyware/Virus Protection
- User's Public Profile
  - Optional/Required by user
  - Seen by other users
  - Email address encrypted
  - Instructions on how to update profile

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

VoIP Privacy and Security Checklist: Security

- Allowing,
  Removing,
  Blocking Callers

- Audit System Activity
  - Server logs
  - Audit Trail

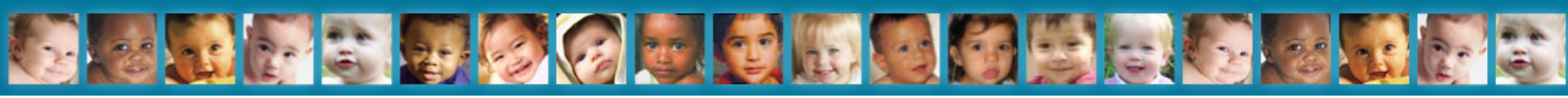
- Security Evaluation
  - Performed by independent group
  - Authentication
  - Password Management
  - Data management
  - Proper security measures

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

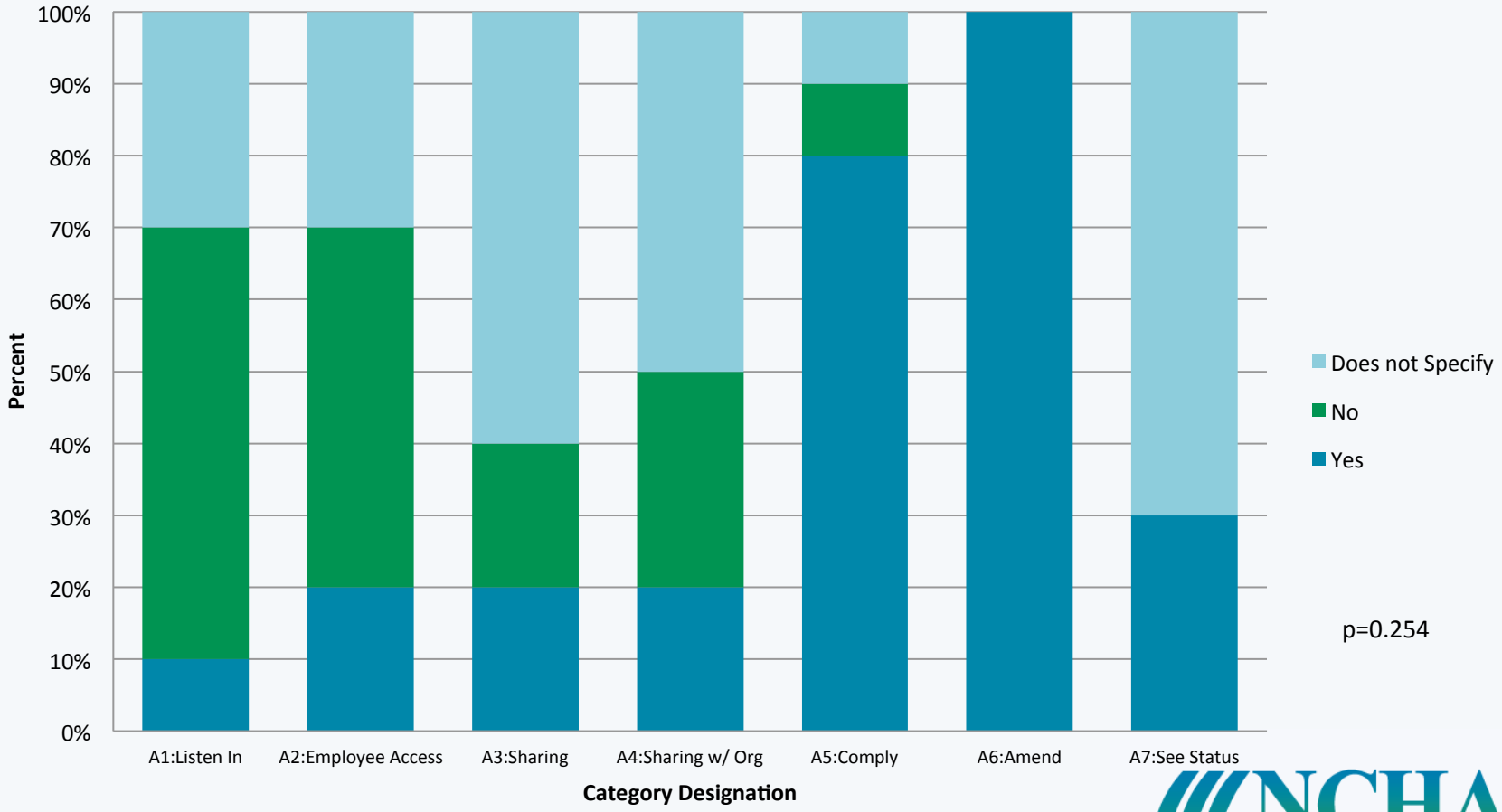
Risk Analysis: Privacy and Security of VoIP

- Risk Analysis of 10 most popular free VoIP videoconferencing software systems was performed
- The top sites were selected from two different websites that reviewed VoIP software systems.
- Each privacy and/or security policy and/or terms of use, whichever was available on the site, was reviewed and analyzed for each of the 58 questions addressed on the checklist.
- A summary of the results of the assessment are provided

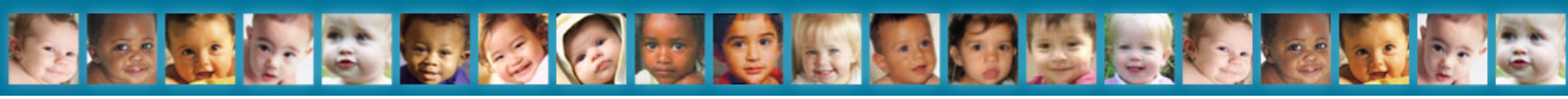
NCHAM
National Center for Hearing Assessment and Management
Utah State University™



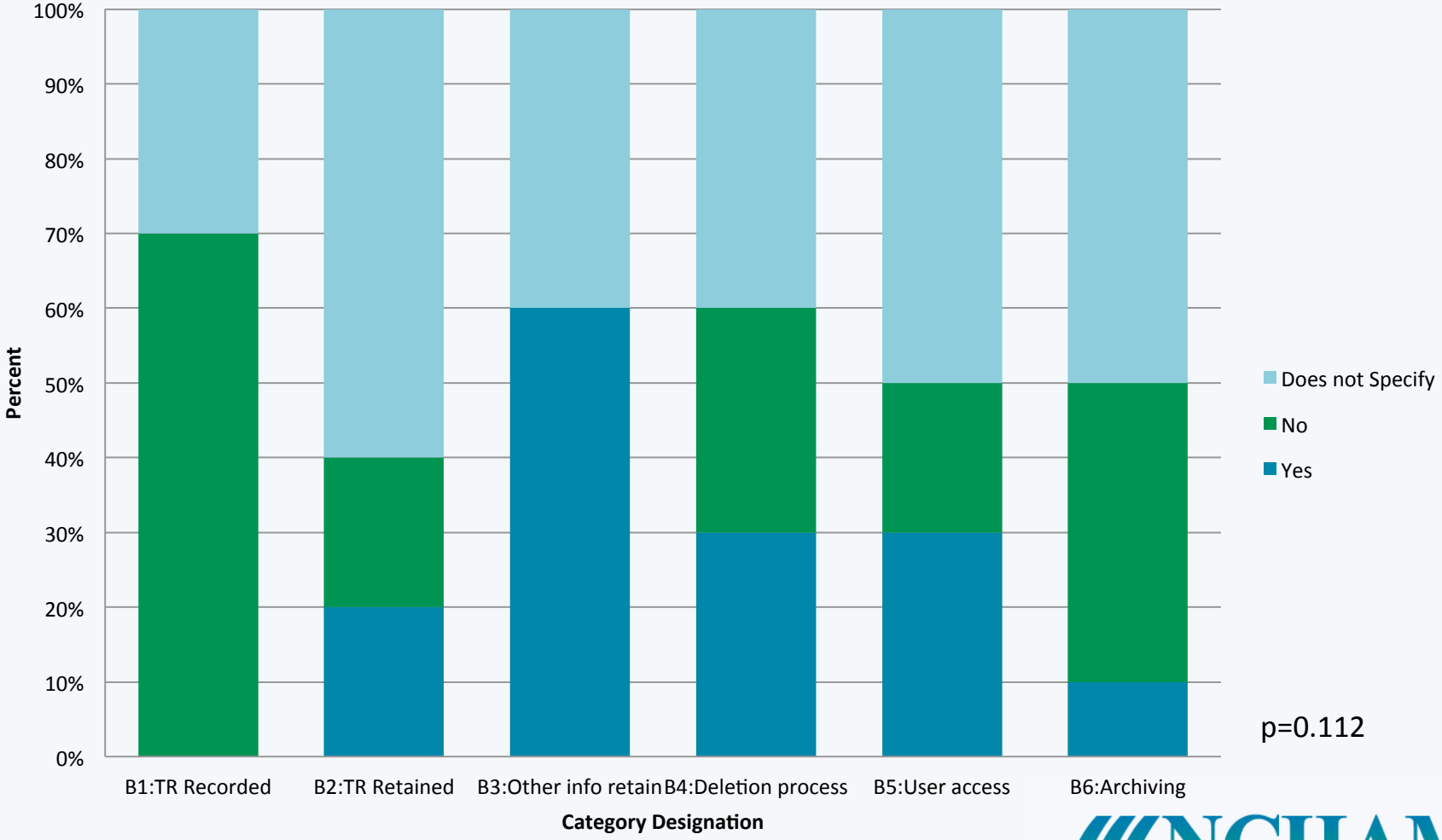
Risk Assessment of Personal Information



NCHAM
National Center for Hearing Assessment and Management
Utah State University™



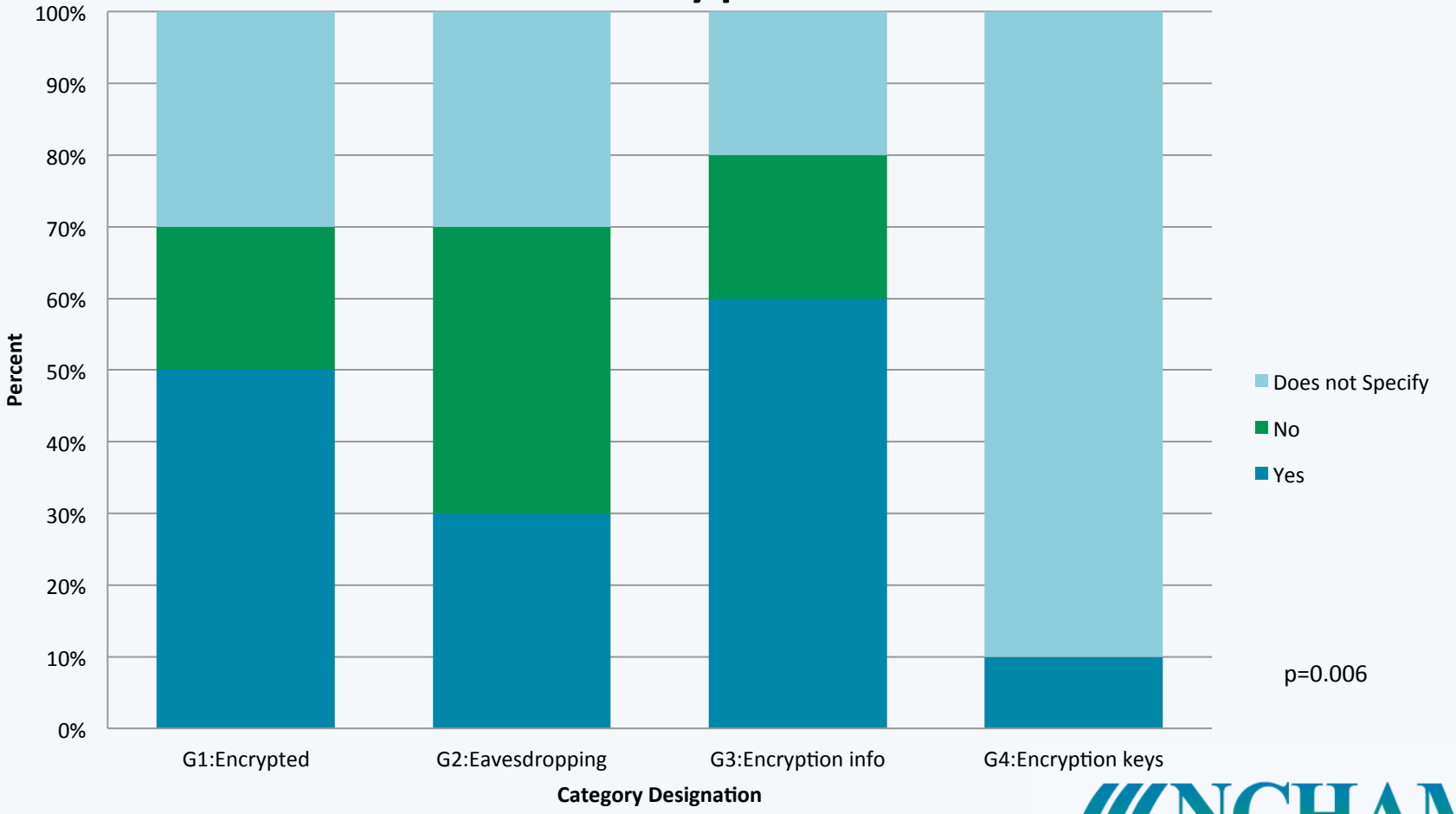
Risk Assessment of Retention of Information



p=0.112

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

Risk Assessment of Security Measures: Encryption

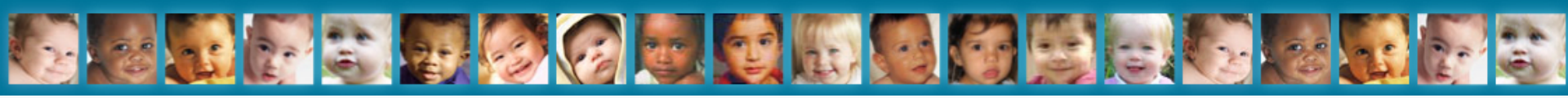


NCHAM
National Center for Hearing Assessment and Management
Utah State University™

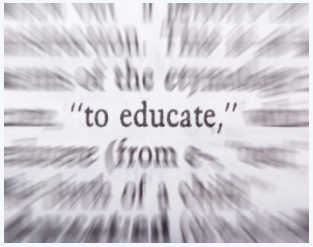
Recommendations

- **Risk Assessment**
- **Use the HIPAA compliance checklist, or, purchase HIPAA compliance software**
- **Form a team of health and legal professionals**
- **Discuss Security Issues**
  - Change default passwords, disable remote access
  - Use two factor authentication when connecting to VoIP server
  - Implement VLAN with stand alone workstations specifically for VoIP transmissions
  - Implement encryption methods

NCHAM
National Center for Hearing Assessment and Management
Utah State University™



Recommendations



- **Educate and train therapists and other rehabilitation personnel**
- **Develop an informed consent**
- **Choose a system that is private and secure --- VISYTER……..**

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

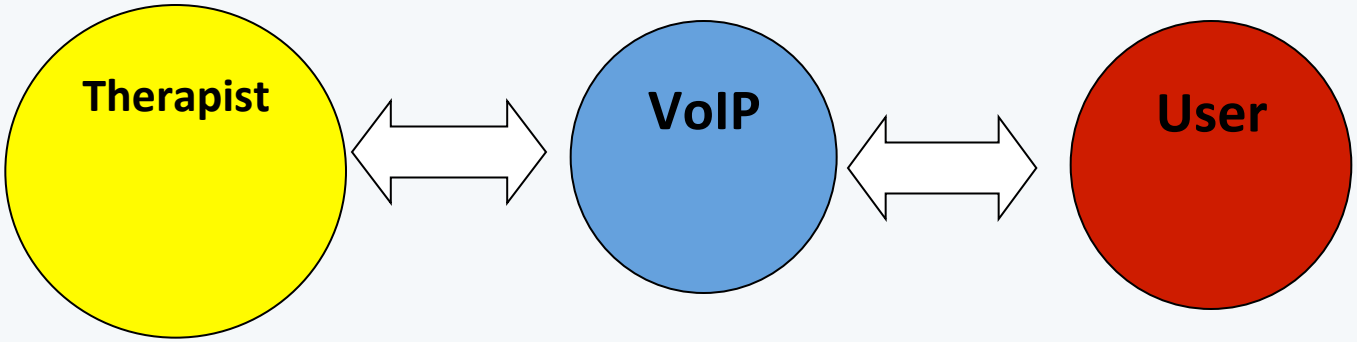
VISYTER—Dr. Bambang Parmanto

- Versatile and Integrated SYstem for TEleRehabilitation (VISYTER) is a software platform for developing various TR applications:
- Including a remote wheelchair prescription, adult autistic assessments, and international physical therapy teleconsultations.
- An evaluation of VISYTER for delivering a remote wheelchair prescription was conducted on 48 participants. Results of the evaluation indicate a high level of satisfaction from patients with the use of VISYTER.
- http://www.youtube.com/watch?v=2cKg7iwD-Ns

NCHAM
National Center for Hearing Assessment and Management
Utah State University™

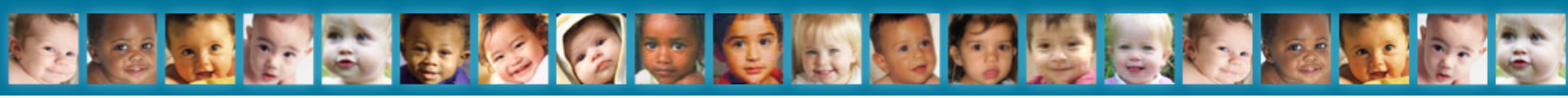
Responsibility

- Open communication and Awareness



- All should examine privacy and security issues

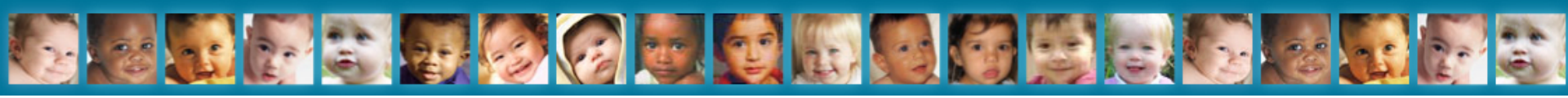
NCHAM
National Center for Hearing Assessment and Management
Utah State University™



Bibliography

- Callahan, J.D., Privacy: The Impact of ARRA, HITECH, and other Policy Initiatives, American Health Information Management Association (AHIMA), 2010
- American Telemedicine Association (ATA), A Blueprint for Telerehabilitation Guidelines, October 2010
- Watzlaf, V., Moeini,S.,Firouzan,P.,VoIP for Telerehabilitation: A Risk Analysis for Privacy, Security, and HIPAA Compliance. *International Journal of Telerehabilitation*, Vol.2, No.2, 3-13.Fall 2010
- Kuhn, D., Walsh T., & Fries S., (2005). Security considerations for voice over IP systems: Recommendations of the National Institute of Standards and Technology (NIST). Technology Administration, U.S. Department of Commerce Special Publication, 800-58.
- Lazzarotti, J., HIPAA Enforcement Regulations Updated for Penalty Increases and Enhancements under the HITECH Act, Retrieved September 9, 2010 from http://www.workplaceprivacyreport.com/2009/11/articles/hipaa-1/hipaa-enforcement-regulations-updated-for-penalty-increases-and-enhancements-under-the-hitech-act/.
- DHHS, HIPAA, CMS Security Series 1-7, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf, 3/2007

NCHAM
National Center for Hearing Assessment and Management
Utah State University™



Questions?

- How does HIPAA differentiate *security* from *privacy*?
- What information can potentially be accessed via Skype?
- Should we expect to eliminate all security risks?
- What is feasible to do in keeping with the spirit of the law?
- What should be contained in a consent form re: risk?
- What more can you tell us about VISYTER and Vidyohealth?
- Has VoIP been classified as a business associate under the HITECH definition (if not, when will this determination be made)?
- What additional resources are available to share with administrators who have concerns related to HIPAA security for VoIP technology?

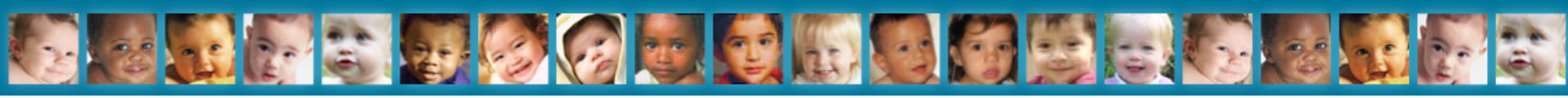
NCHAM
National Center for Hearing Assessment and Management
Utah State University™

Addressing Security at Sound Beginnings:

Daniel Ladner

1. Computer:
   - Password-protected
   - Anti-Virus and Anti-Spyware protected
   - Disallow new program installation
2. Session Recording:
   - Equipment examples
   - Record as digital files or onto DVDs?
   - How are recordings made available to researchers and families ?
3. Software:
   - Data stream encryption and network data nodes; “note passing with secret decoder rings” analogy
   - Central directory service; “unlisted number” analogy
   - Specific examples: Skype (free public service) and Tandberg (purchased private service)
4. External environment
   - Physically locking down equipment
   - Eavesdropping concerns and soundproofing
   - Staff access to equipment
   - Access to session recordings
   - Legal concerns

NCHAM
National Center for Hearing Assessment and Management
Utah State University™



The Role of Consent Forms in Addressing Security

What are critical elements?

- ✓ Simple, clear description of TI/telemedicine
- ✓ Listing of the types of information shared
- ✓ Potential Benefits
- ✓ Potential Risks in security and quality of service
- ✓ Parent signature reflecting understanding of risks, options

NCHAM
National Center for Hearing Assessment and Management
Utah State University™