



HIPAA Privacy & Security

Development Systems, Inc.
Audio Conference
February 24, 2005

[What is confidentiality?]

- Health Insurance Portability and Accountability Act (HIPAA) Privacy & Security Standards
- HIPAA includes 9 references to confidentiality
- *Confidentiality* means that data or information is not made available or disclosed to unauthorized persons or processes
- The focus is on the protected health information - Medical records are not specifically referenced in HIPAA

Confidentiality references - HIPAA

- Ensure the **confidentiality**, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (security)
- Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the **confidentiality**, integrity, and availability of electronic protected health information held by the clinic. (security)

Confidentiality references – HIPAA (continued)

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the **confidentiality**, integrity and availability of the electronic protected health information that it creates, receives, maintains or transmits on behalf of the clinic. (security)
- A parent, guardian, or other person acting *in loco parentis* assents to an agreement of **confidentiality** between a covered health care provider and the minor with respect to such health care service. (privacy)

[HIPAA]

Reminders & Notes

- HIPAA is established as a minimum standard
- Reference should be made to state laws, funding sources, other relevant and applicable resources
- Privacy rule refers to use and disclosure of information, client rights – in any form
- Security standard refers to electronic format only

Protecting information

Electronic

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the clinic creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required [Privacy Rule, 164].
4. Ensure compliance with your workforce.

Protecting information

Electronic

- Flexibility of approach
- Standards
 - Administrative Safeguard
 - Physical Safeguards
 - Technical Safeguards
 - Organizational Requirements
 - Policies, Procedures and Documentation
- Required and addressable

Protecting information

Paper format

- Standard: A clinic may not use or disclose protected health information, except as permitted or required.
- Permitted
 - to the client
 - for treatment, payment, operations
 - other
- Required
 - to clinics when requested
 - compliance

[Policies & Procedures]

■ Assessment

- Re-assess privacy
- Security risk analysis
- Documentation of assessment process

■ Policy development

- Changes in privacy laws documented
- Security policy

■ Staff education

- Changes in policies and notification to staff
- Documentation
- New staff training



Questions?