# Health Care: Privacy & Security in a Digital Age

**HIPAA Summit West**

**Data Security Mini Summit – March 14, 2002**

**Chris Apgar, Data Security & HIPAA Compliance Officer**
**Providence Health Plans**

# Presentation Overview

- Electronic Records & You
- Risks & Valid Concerns
- Legal Protections
- Providence Health Plan - Case Study
- Tips for Protecting Privacy & Security
- Resources
- Q&A



Providence | Health Plans

# Electronic Records & You

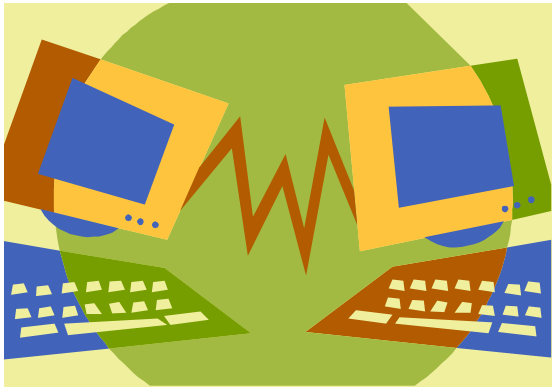
- Health care information users
  - Providers (I.e., doctors, chiropractors, EAP, etc.)
  - Health insurance companies
  - Government & government contractors
  - Third parties (I.e., billing services, medical management, etc.)
- How much control do you really have?
- Marketing, research and other “hidden” uses

# Electronic Records & You

- **Moving information around**
  - **E-mail**
  - **FTP (file transfer protocol)**
  - **Other forms of magnetic media**
  - **US Postal Service and other carriers**
  - **Secure web sites & other forms of secure messaging**
- **Storage and internal organization information transfer**

# Risks & Valid Concerns

- Unprotected Internet
- Web browsing & cookies - tracking your travel
- Authentication or who can look at my record



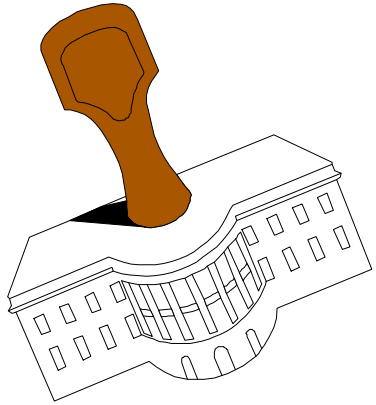
- Networks, firewalls and the lack thereof
- Inappropriate information use for marketing and other sales activities
- Government, courts and data sharing

# Risks & Valid Concerns

- Hackers and other illegal activity
- Internal mischief or the disgruntled employee
- Carelessness or “my record on the counter”
- Lack of physical security (“it’s not locked up”)
- Lack of defined policies, confidentiality practices, etc.

# Legal Protections

- State statute & rule
- Health Information Portability & Accountability Act of 1996 (HIPAA)
- Gram-Leach-Bliley Act
- Children's On-line Privacy Protection Rule
- Other federal statute & rule
- Litigation



# Legal Protections: HIPAA Example

## Data Security

- Risk Assessment
- Policy & procedure development
- Training & awareness
- Contingency Plan
- Information access control ("need to know")
- Audit & certification
- Documentation
- Record access (release management & file access)
- Personnel security & authentication
- Chain of Trust/Business Associate Agreement
- Security & privacy management
- Security incident response
- Physical security

# Providence Health Plan - Case Study

- Security & privacy officers appointed
- Data security & privacy standards developed & implemented
- Staff training & policies developed & communicated
- Use of firewalls and other tools to protect information



Providence | Health Plans

# Providence Health Plan - Case Study

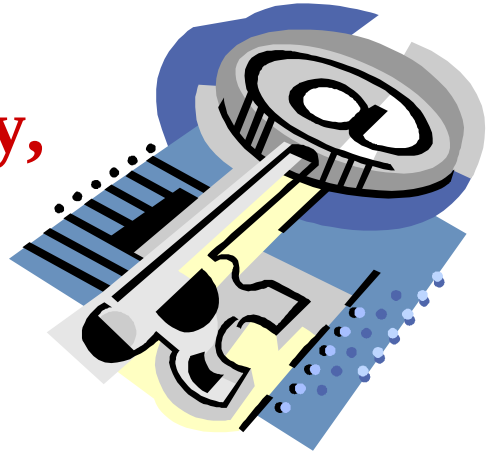
- On-going network & other access point monitoring
- Enforcement of secure transfer of information to authorized staff and external partners
- All accessing confidential information legally bound to enforce privacy & security
- Internal & external audit of policies, training plan & processes

# Providence Health Plan - Case Study

- Collaboration with Providence Health System
- On-going work with external partners (providers, plans, government, etc.)
- Participation in local and national security/ privacy forums
- Privacy & confidentiality - Providence strategic objective

# Personal Tips: Security & Privacy

- Talk to your provider and insurance carrier - what is their privacy policy, how do they protect your confidential health information, etc.)
- Check out web sites (I.e., security, privacy policies, etc.)
- Cookies and what to do with them



# Personal Tips: Security & Privacy

- Avoid sharing health information over unsecured web sites
- Report on-line privacy violations as appropriate
- Avoid unsecured e-mail (even with your provider)

- Periodically request copies of your health record from provider and insurance carrier

# Personal Tips: Security & Privacy

- Carefully read consent & authorization forms (I.e., information release, purpose of confidential data use, etc.)
- Question if in doubt and avoid signing when transmission of your health information not clearly defined
- Know your rights and exercise them

# Resources

- **Federal Trade Commission: http://www.ftc.gov**
- **HIPAA Web Site: http://aspe.hhs.gov/admnsimp**
- **National Institute of Health (regulatory information): http://list.nih.gov**
- **“Defend Your Medical Data” (ACLU): http://www.aclu.org/action/medregs/readstories.html**

# Resources

- **Health Privacy Project: http://www.healthprivacy.org**
- **Department of Health & Human Services Office of Civil Rights: http://www.os.dhhs.gov/ocr/hipaa**
- **American Medical Association: http://www.ama-assn.org**

# Resources

- American Psychology Association on Privacy: http://helping.apa.org/dotcomsense
- Providence (see privacy statement): http://www.providence.org
- Google (search engine; advanced search on “privacy health” or “security health”): http://www.google.com

# Question & Answer

**Chris Apgar, Data Security &**
**HIPAA Compliance Officer**
**Providence Health Plan**
**3601 SW Murray Blvd., Suite 10**
**Beaverton, OR 97005**
**(503) 574-7927 (voice)**
**(503) 574-8655 (fax)**
**apgarc@providence.org**