TEPR

Voluntary Universal Identifier – Pipe Dream or Panacea?

Wednesday May 21, 2008

Deborah C. Peel, MD

patientprivacyrights

Definition of Privacy

“Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.”

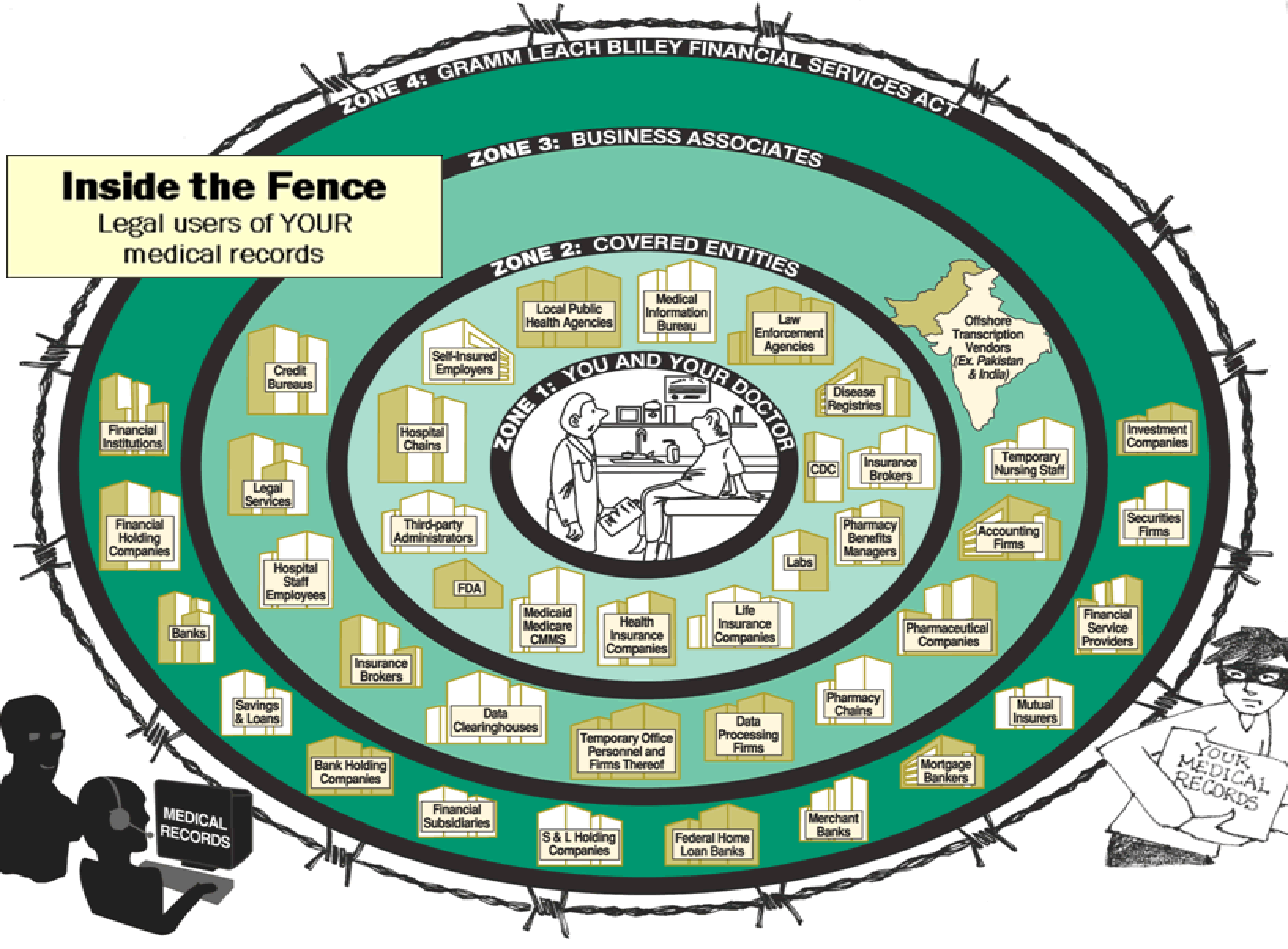
NCVHS Report to Sec Leavitt, June 22, 2006

The elimination of consent and privacy

1996	Congress passed the HIPAA statute, instructing the Dept. of Health and Human Services (HHS) to make address Americans' rights to health information privacy.	*"Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to [Congress]…**detailed recommendations on standards with respect to the privacy of individually identifiable health information."***
2001	President Bush implemented the original HIPAA "Privacy Rule" recognizing the "right of consent".	*"….a covered health care provider **must obtain the individual's consent,** in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations."*
2002	Amendments to the "Privacy Rule" eliminated the "right of consent".	*"The **consent provisions…are replaced** with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations."*

Inside the Fence

Legal users of YOUR medical records



The future without privacy

- **Job loss/ denial of promotions**
  - People are judged on health information, not qualifications, abilities, or experience
- Tsunami of identity theft/medical identity theft
- Insurance discrimination
- Credit denial
- Denial of admission to schools
- Marketing
- *New classes of citizens who are unemployable and uninsurable*

Privacy and identity systems

- Single identifiers/centralized ID systems
  - History
  - Problems
- Metasystems of identification
- VUHID system
- Privacy solutions for electronic health systems and HIE

Americans Have Consistently Rejected National ID Systems

Single identifiers/centralized systems

1936 When the Social Security Number (SSN) was created it was meant to be used only as an account number associated with the administration of the Social Security system.

Though use of the SSN has expanded considerably, it is not a universal identifier and efforts to make it one have been consistently rejected.

Single identifiers/centralized systems

1973 “We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems.”

Dept of Health, Education, and Welfare, Sec’y’s Advisory Comm. On Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (July 1973), available at www.epic.org/privacy/hew1973report/.

1977 The Carter Administration reiterated that the SSN was not to become an identifier.

Single identifiers/centralized systems

1981 In Congressional testimony Attorney General William French Smith stated that the Reagan Administration was “explicitly opposed to the creation of a national identity card.”

1996 HIPAA Statute requires a national system of UPINs. Led by Rep Ron Paul, Congress refuses to fund the system due to voter opposition.

Single identifiers/centralized systems

2004 "[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card. The citizens of the United States have consistently rejected the idea of a national identification system."

Tom Ridge, Sec'y **Department of Homeland Security**, Address at the Center for Transatlantic Relations at Johns Hopkins University: "Tansatlantic Homeland Security Conference" Sept 13, 2004, www.dhs.gov/xnews/speeches/speech_0206.shtm.

2008 REAL ID

Civil liberties advocates and the states oppose imposition of REAL ID

Privacy problems with single identifier systems

- Americans do not want single identifiers
- One primary ID for most health data = loss of data

Expanded data collection and retention increases security risks

- Increase risk of privacy breaches
- Increase risk of ID theft
- Increases risk of fraud
- Increases risk of authorized users abusing power
- Increases scope of harm (millions of records can be breached)

Identity metasystems

- Limit risk of ID theft by distributing identity—use different profiles in different authenticating contexts
- Limit scope of breaches or misuse to a single context and data set, ex: a single bank account or merchant account or medical record
- Limit risk of breaches because smaller systems = less valuable targets, contain less identifying data

Problems with VUHID identifiers

- Designed for RHIOs and HIEs
  - Information sharing policies in RHIOs and HIEs are NOT set by the individual = loss of privacy/autonomy (control over access)
  - Cannot segregate sensitive data at a granular level = loss of privacy
- One primary identifier (OVID) for most health data = high risk for loss of privacy
- Multiple PVIDs are needed for sensitive data = complex
- OVID + many PVIDs = fat wallet filled with cards,
- Have to write on cards to identify class of data = loss of privacy
- “Open” IDs are a bad idea (all health data is sensitive)

Problems with VUHID identifiers

- Data scattered across many databases = high security and privacy risk
- Multiple databases exist with OVIDs and PVIDs linked to EMPIs = loss of privacy
- VUHID does not know which person is associated with which ID, but everyone else does
- Physicians and EMPIs both know which person is associated with which ID = loss of privacy, high risk for theft
  - Physicians have demographic and clinical data linked to OVIDs and PVIDs
  - EMPIs have demographic data linked to OVID and PVIDs

VUHID privacy implications

- VUHID is dangerous to privacy for the same reason it is useful--it facilitates linking disparate information
- VUHID is unnecessary for health information infrastructure (health banks, IDs that only operate at banks, and independent consent management tools)

Privacy Solutions

- No centralized ID systems
- Robust 2nd factor authentication or authentication that preserves anonymity
- No third party collection or storage of ID data
- Authentications must be kept separate and distinct from all individually identifiable information
- No biometrics used for IDs
- Health banks/consent management tools
- Cubbyhole database architecture

Americans Want Privacy

The Coalition for Patient Privacy, 2007

AIDS Action
American Association of People with Disabilities
American Association of Practicing Psychiatrists
American Chiropractic Association
American Civil Liberties Union
American Conservative Union
American Psychoanalytic Association
Association of American Physicians and Surgeons
Bazelon Center for Mental Health Law
Bob Barr (former Congressman R-GA)
Citizens for Health
Citizen Outreach Project
Clinical Social Work Association
Consumer Action
Consumers for Health Care Choices
Cyber Privacy Project
Doctors for Open Government
Ethics in Government Group
Fairfax County Privacy Council
Family Research Council
Free Congress Foundation
Georgians for Open Government
Gun Owners of America
Health Administration Responsibility Project, Inc.
Just Health
Multiracial Activist
Microsoft Corporation Inc.
National Center for Transgender Equality
The National Center for Mental Health Prof. & Consumers
National Whistleblower Center
National Workrights Institute
Natural Solutions Foundation
New Grady Coalition
Pain Relief Network
Patient Privacy Rights Foundation
Privacy Activism
Privacy Rights Now Coalition
Private Citizen, Inc.
Republican Liberty Caucus
Student Health Integrity Project
TexPIRG
Thoughtful House Center for Autism
Tolven, Inc.
Tradition, Family, Property, Inc.
Universata, Inc.
U.S. Bill of Rights Foundation
You Take Control, Inc.

2007 Privacy Principles

Coalition for Patient Privacy

- **Recognize that patients have the right to health privacy**
  - Recognize that user interfaces must be accessible so that health consumers with disabilities can individually manage their health records to ensure their health privacy.

- The right to health privacy applies to all health information **regardless of the source, the form it is in, or who handles it**

- Give patients **the right to opt-in and opt-out** of electronic systems
  - Give patients the right to segment sensitive information
  - Give patients control over who can access their electronic health records

- Health information **disclosed for one purpose may not be used for another purpose** before informed consent has been obtained

- Require **audit trails** of every disclosure of patient information

2007 Privacy Principles

Coalition for Patient Privacy

- Require that **patients be notified promptly** of suspected or actual privacy breaches
- **Ensure that consumers can not be compelled to share health information** to obtain employment, insurance, credit, or admission to schools, unless required by statute
- **Deny employers access** to employees’ medical records before **informed consent** has been obtained
- Preserve stronger privacy protections in **state laws**
- **No secret health databases.** Consumers need a clean slate. Require all existing holders of health information to disclose if they hold a patient’s health information
- Provide **meaningful penalties and enforcement mechanisms** for privacy violations detected by patients, advocates, and government regulators

What Can You Do?

- Sign up for e-alerts at www.patientprivacyrights.org
  - *Stay informed, take action*
- Patient Privacy Toolkit www.patientprivacyrights.org
  - What to ask your doctors and providers
  - Use consent forms that preserve privacy
- Use ‘smart’ HIT products and systems that ensure privacy
- Look for ‘smart’ privacy certification seal
- Support ‘smart’ legislation
  - TRUST Act HR 5442, IHRT Act HR 2991

Coming soon….
PrivacyRightsCertified, Inc.

The ***Privacy Rights Certified*** seal certifies privacy and security at the highest international privacy standards, guaranteeing that patients control all access to their health information.

Privacy Rights Certified is the first and only independent certification seal for health technology—uninfluenced by government or business interests.

‘Smart’ privacy and security solutions

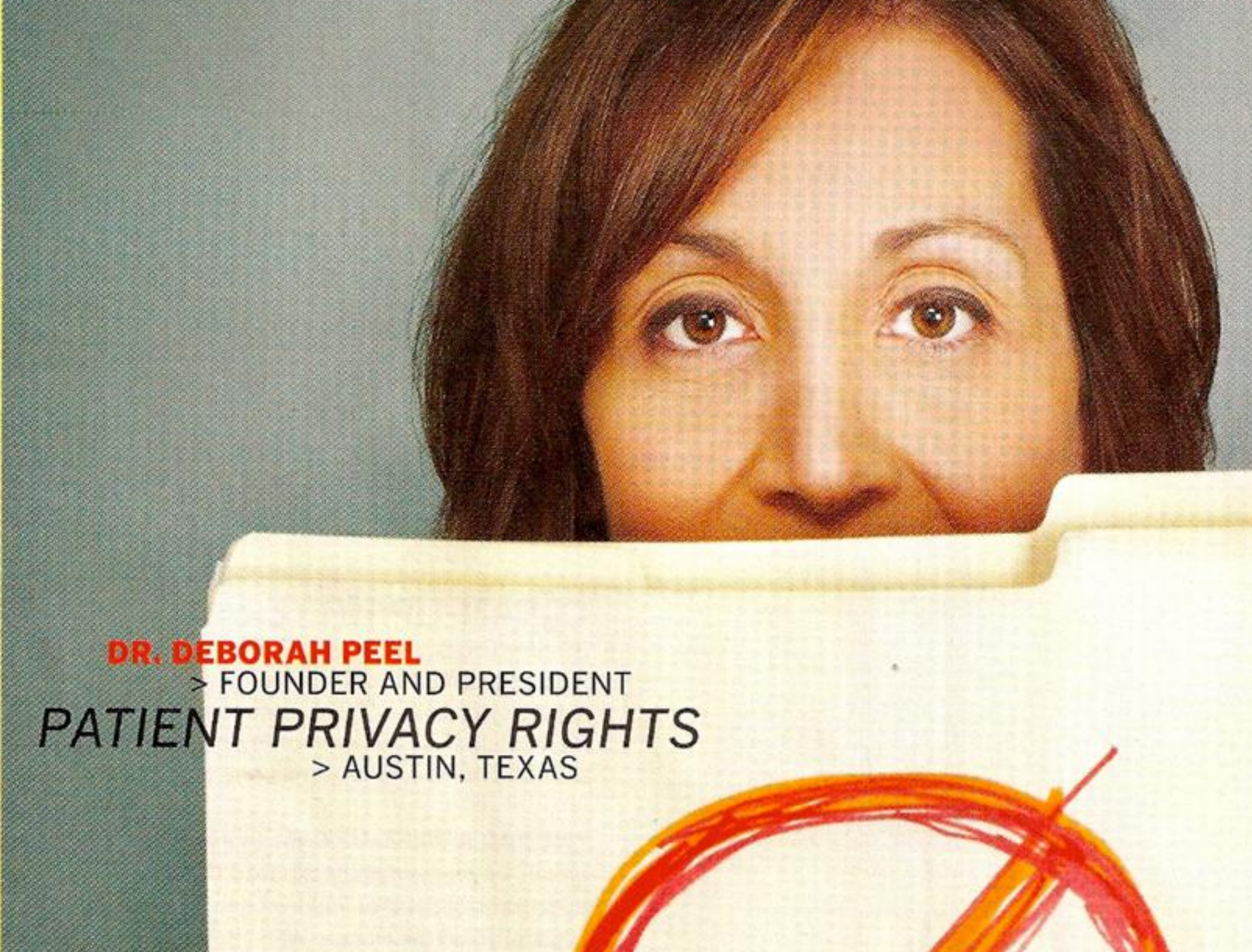
‘Smart’ certification

PrivacyRightsCertified

Consumer-led organization offering a Good Housekeeping Privacy Seal-of Approval for HIT systems and products that ensure consumer control of PHI

Privacy Rights Certified will ensure Americans **UNDERSTAND** PHRs and EHRs,**CHOOSE** wisely, and take steps to **PROTECT** their most intimate information.

- Continually updates standards to address new and emerging threats to privacy, security, and confidentiality
- Assures legal compliance with the most stringent state, federal, and international privacy laws and rights.
- Governed by leading national consumer and privacy organizations and experts



DR. DEBORAH PEEL
> FOUNDER AND PRESIDENT
PATIENT PRIVACY RIGHTS
> AUSTIN, TEXAS

Will you join with us?

www.patientprivacyrights.org

Deborah C. Peel, MD
Founder and Chair
dpeelmd@patientprivacyrights.org

Ashley Katz, MSW
Executive Director
akatz@patientprivacyrights.org

512.732.0033 (office)