Privacy & Data Protection

1

Disclosures

- None

2

K Royal, JD, PhD, FIP, CIPP/US /E, CIPM, CDPSE
kroyal@heartofprivacy.com

- Licensed attorney in Arizona and Fellow of Privacy with IAPP
- Over 25 years of experience in the legal and medical fields
- Featured author for privacy with Association of Corporate Counsel
- Co-host of the podcast **Serious Privacy**
- Teach Privacy and Emerging Technology at ASU College of Law
- Was a nurse when HIPAA was passed….

What we're covering today

Introduction

Your Obligations

The Legal Side

Key Issues

Introduction
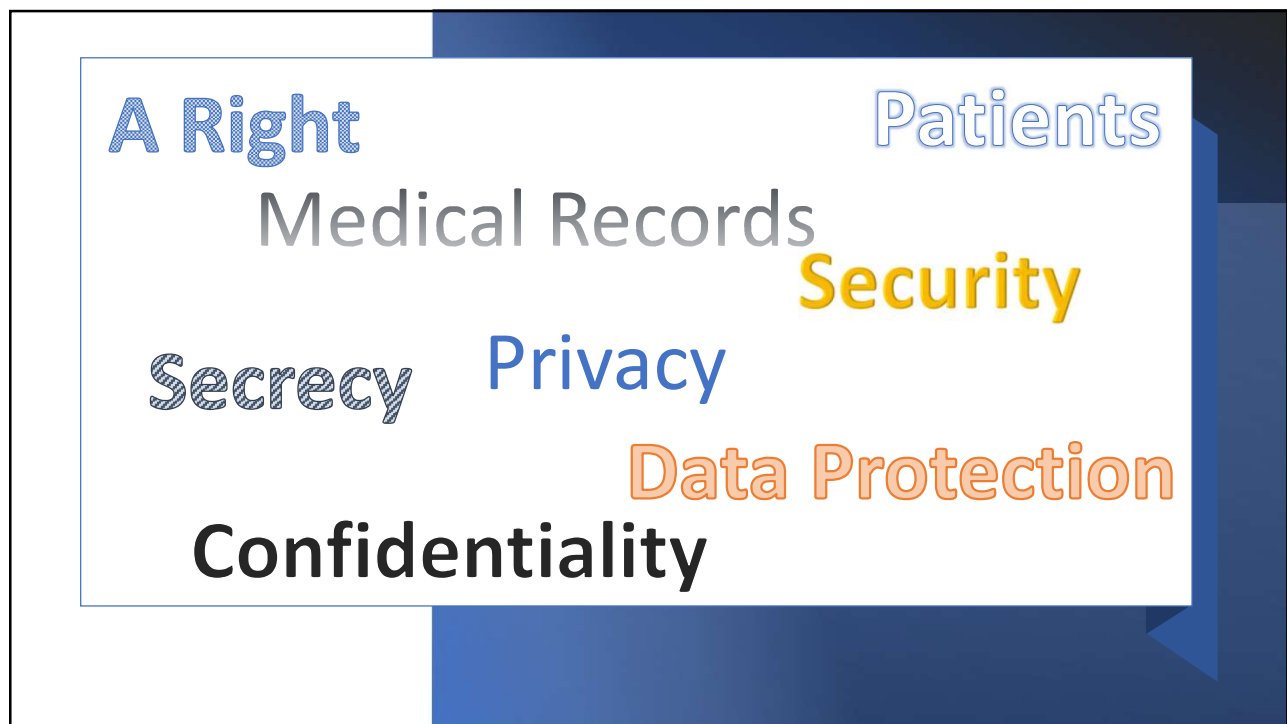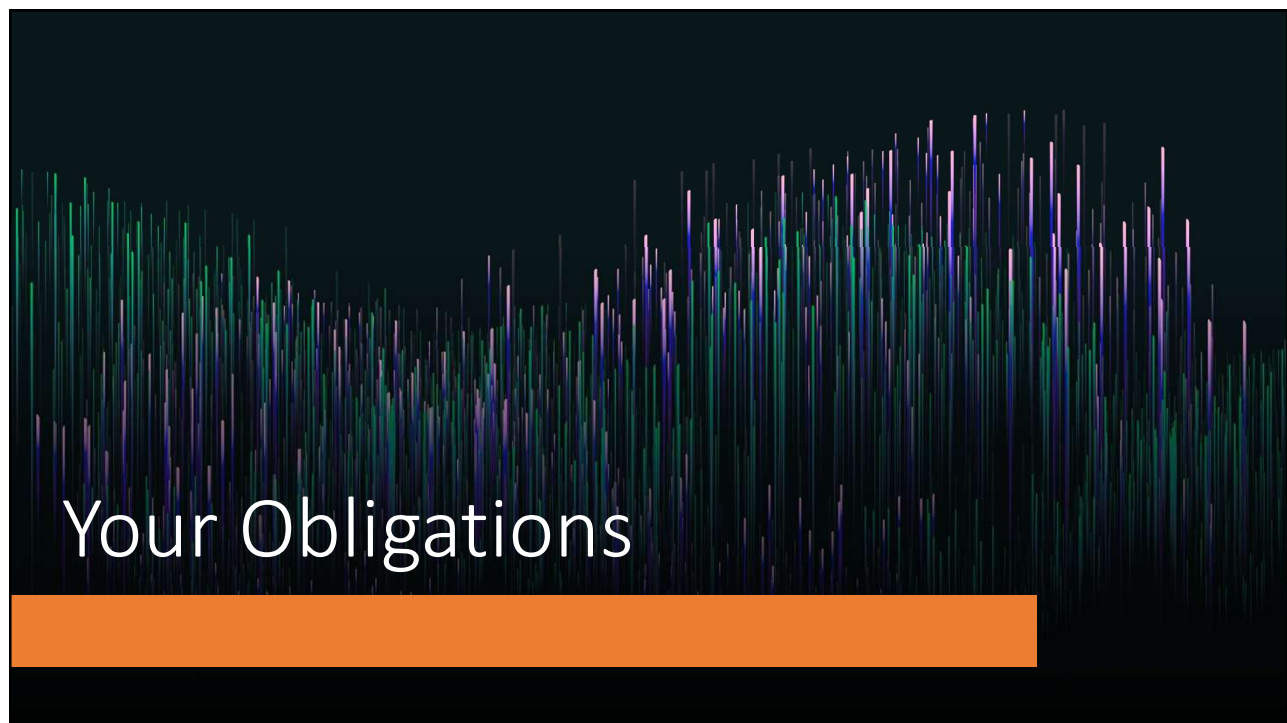
What do you think of when you hear "privacy"?

A Right

Patients

Medical Records

Security

Secrecy

Privacy

Data Protection

Confidentiality

Your Obligations

Doctors of Osteopathy

Ethical obligations

Practice requirements

The Legal Side

11

HIPAA

- Health Insurance Portability and Accountability Act of 1996
  - Privacy Rule 2003
  - Security Rule 2005
- Amended by HITECH Act (Health Information Technology for Economic and Clinical Health Act) of 2009
  - Final implementation date was in 2013
  - Breach Notification Rule
  - Applicable to business associates

12

Business Associates

Access, Collect Protected Health Information on your behalf

May want to use portions of the data for their own purposes

Recommendations

Do your due diligence

Put the agreement in place

Know who they use

Information Blocking Rule

- On June 27, 2023, HHS-OIG posted its final rule implementing information blocking penalties. The final rule establishes the statutory penalties created by the 21st Century Cures Act. If OIG determines that an individual or entity has committed information blocking, they may be subject up to a **$1 million penalty per violation**.

- **Enforcement.** Enforcement of the information blocking penalties began September 1, 2023. OIG will not impose a penalty on information blocking conduct occurring before September 1, 2023.

- The final rule does not impose new information blocking requirements. OIG incorporated regulations published by the Office of the National Coordinator for Health Information Technology (ONC) as the basis for enforcing information blocking penalties. For more information on ONC's information blocking regulations see: Information Blocking.

- To report complaints about information blocking, please visit the ONC Information Blocking Portal or the OIG Hotline.

Information Blocking

Definition: `information blocking' means a practice that--

(A) except as required by law or specified by the Secretary pursuant to rulemaking under paragraph (3), is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and

(B)(i) if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or

(ii) if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

FAQs on providers

- Information blocking rules apply whether or not providers use certified health IT.
- For purposes of the information blocking regulation, a "health IT developer of certified health IT" is defined in 45 CFR 171.102. With the sole exception of a health care provider that self-develops certified health IT for their own use, this definition is met by any individual or entity that develops or offers health IT certified under the ONC Health IT Certification Program.

- See Information Blocking Actions fact sheet
- https://www.healthit.gov/cures/sites/default/files/cures/2020-03/InformationBlockingActors.pdf

State Laws – Omnibus Privacy laws

Currently in Effect
- CA, CO, CT, VA
- UT goes into effect end of 2023

Passed this year
- DE, IN, IA, MT, OR, TN, TX
- FL – high tech

All have privacy rights
- Access, Deletion

All have definitions of sensitive personal data

Sensitive Health Information - Culture

Key Issues

Artificial Intelligence

21

Telehealth

Update	Update your privacy and security practices and your notice with patients
Use	Use applications that are HIPAA-compliant
Turn on	Turn on all the available encryption and privacy modes
Manage	Manage mobile device access
Limit	Limit network access
Enable	Enable multifactor authentication on everything possible
Maintain	Maintain good cyber hygience

22

Data Breaches

- HIPAA
  - Breach listings
    https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- State law
- Private lawsuits / Class action lawsuits
- AG enforcement

Questions

kroyal@heartofprivacy.com