MARYLAND HEALTH CARE COMMISSION

HIPAA Privacy & Maryland Requirements

HIPAA
Requirement Review & Reminder

The Health Insurance Portability and Accountability Act of 1996, Administrative Simplification, requires payers, providers, and claims clearinghouses to establish protections, adopt standards, and meet requirements for the transmission, storage, and handling of certain health care information.

HIPAA Exemptions Exist But May Have Long-Term Implications

- A provider of services with fewer than 25 full-time equivalent employees
- A physician, practitioner, facility, or supplier with fewer than 10 full-time equivalent employees
- No EDI

Overall Compliance…
Aim For The "Bull's Eye"
Ongoing Efforts Likely To Continue

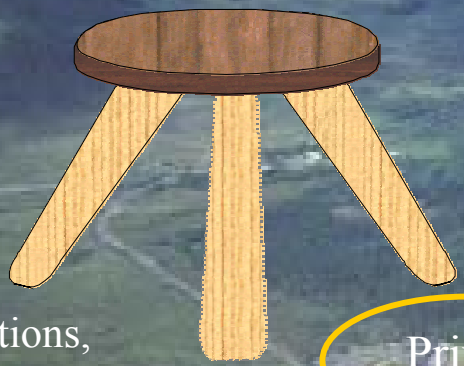
Transactions, Code Sets, Identifiers – October 16, 2003

Privacy – April 14, 2003

Security – April 21, 2005

Administrative Simplification

Future Regulations Pending



Transactions,
Code Sets,
Identifiers

Security

Privacy


Did You Know...
Maryland Has A Privacy Law...
"Maryland Confidentiality
of Medical Records Act"

Maryland Confidentiality of Medical Records Act - Background...

- 1978 Maryland Medical Records Act
- 1990 Confidentiality of Medical Records Act
  - 1984 - 22 page report identified discrepancies in medical records confidentiality
  - 1987 - Attorney General redrafts confidentiality law for mental health records
  - 1989 - Health Subcommittee, of the Senate Economic and Environmental Affairs Committee drafts a detailed statutory coverage of confidentiality of medical records
  - Senate Bill Number 584 signed into law on May 29,

Maryland Confidentiality of Medical Records Act Compared To HIPPA's Privacy Regulations

"Some Say HIPAA Privacy Has Been In Maryland For Nearly 12 Years…"

HIPAA Privacy
Federal/State Comparison

True or False: HIPAA is a national effort to standardize the storage, transmission, and handling of certain patient information

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Business Associate Agreements	**(H)** √ contracts are required when sharing patient information with a non-covered entity. **(S)** does not require written agreements, however, certain redisclosure provisions apply.
Coroners	**(H)** allows for disclosure to medical examiners. **(S)** √ limits disclosure of the medical and psychological information to relevant purpose.

HIPAA Privacy
Federal/State Comparison

True or False: HIPAA is scalable to all covered entities

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Covered Entities	**(H)** limited to EDI activity of payers, providers, and claims clearinghouses. **(S)** √ covers all health care providers – not limited to just EDI.
Covered Information	**(H)** √ medical record, financial record and 19 individual identifiers. **(S)** limited to information contained in the medical record.

HIPAA Privacy
Federal/State Comparison

True or False: HIPAA - Sound documentation is essential…

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Deceased & Autopsy Reports	**(H)** deceased individuals information protected, limited to intended purpose. **(S)** √ strong protections exist for deceased individuals - special administrative rules apply to autopsy.
Disclosures - Abuse & Neglect	**(H)** allows for providers to report instances of suspected abuse. **(S)** √ compels providers to disclosure information of suspected abuse.

HIPAA Privacy
Federal/State Comparison

True or False: HIPAA enforcement should be viewed more as "a carrot and not a stick"

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Disclosures – Family, Friend, Etc.	**(H)** practitioner discretion unless advised otherwise by patient. **(S)** similar to federal requirements.
Disclosures - Legally Compelled	**(H)** allows when required by regulation (law). **(S)** √ defines specific types of compelled disclosures, i.e., subpoena, summons, warrant, or court order.

HIPAA Privacy
Federal/State Comparison

True or False: CMS monitors the privacy regulations and OCR monitors the transaction & code set standards

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Disclosure - Mandatory v. Permissive	**(H)** no direct provision, rather it's implied. **(S)** √ outlines elements for mandatory disclosure. Protections exist against litigation based on a technical violation.
Disclosure - Minimum Necessary	**(H)** √ only allowed to disclose minimum amount of information to accomplish task. **(S)** strong protections apply to mental health record disclosures.

HIPAA Privacy
Federal/State Comparison

True or False: The medical record, financial record, and 19 identifiers make up PHI

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Disclosure - Patient Consent	**(H)** allows for disclosure of patient information to carry out treatment, payment, and health care operations. **(S)** disclosure allowed to resolve claims-adjudication and other related issues.
Disclosures – Permissive	**(H)** √ allows disclosures for treatment, payment, and health care operations permissive. **(S)** permits most disclosures necessary for health care operations.

HIPAA Privacy
Federal/State Comparison

True or False: Providers may not use professional judgment to make reasonable inference of an individuals best interest

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Disclosures - Public	**(H)** √ limits use to regulatory authority, certain data to law enforcement, and funeral directors. **(S)** prohibits disclosure of medical or psychological information except for autopsy or in other well-defined situations.
Disclosures - Public Health	**(H)** √ details the type of information for disclosure in matters of public health. **(S)** allows for disclosure for purposes of investigation or treatment.

HIPAA Privacy
Federal/State Comparison

True or False: Providers must obtain a written authorization for all marketing activities

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Disclosures - Public Safety Threat	**(H)** allows disclosures to lessen threat to a person or the public. **(S)** allows authorities to perform lawful duties. Both are very similar in nature.
Disclosures - Specialized Government Functions	**(H)** √ allows disclosures covering military personnel, security, and protective services. **(S)** allows authorities to perform investigative duties.

HIPAA Privacy
Federal/State Comparison

True or False: Individuals must approve all uses and disclosures of PHI

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Disclosures - Worker's Compensation	**(H)** allows disclosures for administration of Worker's Compensation programs. **(S)** injured employee authorizes disclosure by filing a claim.
Electronic Claims	**(H)** uses EDI as a core component for a health care provider to be considered a covered entity. **(S)** √ health care providers are covered entities whether or not they use EDI.

HIPAA Privacy
Federal/State Comparison

True or False: Providers must make reasonable attempts to accommodate requests to receive PHI by an alternative means

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Elements of Patient Consent	**(H)** √ informs patients about use of their medical information, refers to the notice of privacy practices, permits patient to request restrictions on access to the medical record. **(S)** consents are not specifically defined.
Emergency Treatment	**(H)** √ may treat in emergency situations, must make a good faith attempt to obtain consent or provide notice of privacy practices. **(S)** allows for professional judgment in emergency situations.

HIPAA Privacy
Federal/State Comparison

True or False: Consents are not optional and must be obtained each time a patient receives treatment

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Employer Access	**(H)** allows access for work-related illness issues. **(S)** √ access is by authorization, in certain situations, employer access can be mandatory. State law provides a broader protection to employees regarding employer access to their medical records.
Enforcement	**(H)** Office of Civil Rights enforces privacy. **(S)** DHMH, licensing boards, disciplinary agencies all can handle enforcement. Both have a similar enforcement structure.

HIPAA Privacy Federal/State Comparison

True or False: Authorizations are more detailed and specific than a consent

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Facility Directories	**(H)** unless objected to-- general patient information may be disclosed. **(S)** may disclose unless instructed not to disclose.
Good Faith Immunity	**(H)** √ allows for provider discretion and use of common practices in decision-making. **(S)** enables providers to use judgment.

HIPAA Privacy
Federal/State Comparison

True or False: Individuals do not have the right to adequate notice of the uses and disclosures of PHI

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Government Access	**(H)** √ allows federal access for public health and enforcement related issues. **(S)** allows for regulatory compliance and reporting.
Health Oversight Activities	**(H)** permits disclosure to health oversight agencies. **(S)** √ compels disclosure for health disciplinary oversight.

HIPAA Privacy
Federal/State Comparison

True or False: Notice of Privacy Practices must be distributed, posted, and made available in provider offices

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Judicial & Administrative Proceedings	**(H)** allows for disclosure by court order or by subpoena upon establishing authentication of the request. **(S)** √ compels disclosure for compliance with judicial requests.
Law Enforcement Investigation	**(H)** allows for compliance with formal investigative process. **(S)** √ state law compels disclosure.

HIPAA Privacy
Federal/State Comparison

True or False: Notice of Privacy Practices cannot be summarized

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Law Enforcement *Public Emergency*	**(H)** permits disclosures. **(S)** allows government agencies to perform investigative duties.
Marketing	**(H)** √ permits marketing of wellness-related services, or generally with a signed authorization. **(S)** providers can use discretion in marketing medical services, equipment, and programs.

HIPAA Privacy
Federal/State Comparison

True or False: Provider must permit individual access to PHI within 30 of the request

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Mental Health Records	**(H)** psych notes protected, authorization required for release. **(S)** √ criteria exists for the disclosure and redisclosure of mental health records.
Minors	**(H)** yields to state law. **(S)** √ minors consenting to treatment have control over their medical records.

HIPAA Privacy
Federal/State Comparison

True or False: Providers must always grant individuals access to PHI

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Monitoring of Released Information	**(H)** √ must act if notified of a Business Associate violation. **(S)** redisclosure is generally limited to health care operations, legal counsel, education, and facility accreditation. Providers are not required to monitor released information.
Oral Communication	**(H)** and **(S)** similarly permit and protect health care communications.

HIPAA Privacy
Federal/State Comparison

True or False: Patient files are not required to be secured

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Patient Access	**(H)** √ access and comments allowed under certain circumstances. Providers own record, patient owns information. **(S)** providers play an active role in deciding patient access and making changes in the medical record.
Patient Authorization	**(H)** √ eight well-defined components of a valid authorization. **(S)** five elements outlining general usage parameters.

HIPAA Privacy
Federal/State Comparison

True or False: Providers are required to guarantee the protection of PHI against all forms of assault

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Patient Consent - Treatment, Payment & Health Care Operations	**(H)** √ signed consent is required for treatment, payment, and health care operations, or a process that includes patient's acknowledgment of the notice of privacy practices. **(S)** express consent not required to treat.
Penalties – Civil	**(H)** √ has strong civil penalties for non-compliance. **(S)** no public civil enforcement penalties, limited to only actual damages.

HIPAA Privacy
Federal/State Comparison

True or False: HIPAA does not require providers to use a sign in sheet

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Penalties – Criminal	**(H)** known acquisition or disclosure - $50,000 and 1 year imprisonment; false pretenses $100,000 and 5 years imprisonment; intent to harm $250,000 and 10 years imprisonment. **(S)** penalties are virtually the same.
Preemption Law	**(H)** and **(S)** law preemption determination is generally based upon the more stringent requirement. In the area of minors, state law prevails.

HIPAA Privacy
Federal/State Comparison

True or False: Individuals do not have the right to inspect and review PHI

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Preemption Law - Secretarial Exemption Process	**(S)** may request federal HIPAA exemption(s) when conflicting state law is required to address specified state need.
Presumption of Confidentiality	**(H)** implied throughout the privacy regulations. **(S)** confidentiality requirements are core to the Act. Both are similar in nature.

HIPAA Privacy
Federal/State Comparison

True or False: Individuals have the right to an accounting of PHI disclosures

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Privacy Officer	**(H)** √ identify a privacy officer, this individual is responsible for implementing the privacy regulations. **(S)** implied that someone makes discloser determinations, establishes and maintains policies and procedures.
Record Retention	**(H)** √ six years – administrative information. **(S)** five years except for minors, then age 18 plus three years.

HIPAA Privacy
Federal/State Comparison

True or False: A business associate acts on behalf of a provider in conducting activities involving use of PHI

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Research	**(H)** authorization required except if approved by a privacy board or an IRB. **(S)** allows use of non-identifying information subject to an IRB review. Both are similar in nature.
Telemedicine	**(H)** allows for communication among health care providers – HIPAA was never intended to impede care. **(S)** requirements are nearly the same as the federal requirements.

HIPAA Privacy
Federal/State Comparison

True or False: Providers are not responsible for actions of a business associate

Category	***Comparison*** ***(H) HIPAA (S) State √ More Stringent***
Transplant	**(H)** permits disclosures for purposes of organ donation. **(S)** allows disclosure for purposes of evaluating possible donations. Both are similar in nature.

HIPAA Privacy

Some Key Items To Remember...

What Really Is Considered Protected Healthcare Information

- Protected Health Care Information (PHI) is defined as:

  Individually identifiable health care information created or received by a provider, payer, or claims clearinghouse related to health condition, provision of health care, or payment for health care

  The final rule was extended in scope to include the protection of all individually health information in any form, electronic or non-electronic, that is held or transmitted by a covered entity. This includes PHI in paper records that never have been electronically

Protected Health Information (PHI)
The 19 Identifiers - Privacy

- Name
- Address
- E-mail
- Dates
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate Number
- License Number
- Vehicle Identifiers
- Facial Photographs
- Telephone Numbers
- Device Identifiers
- URLs
- IP Addresses
- Biometric Identifiers
- Geographic Units
- Any Other Unique Identifier Or Codes

Remember - Provider Discretion Is Preserved Under HIPAA

"A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protect health care information."

- Page 44 (3) Limited uses and disclosures when the individual is not present, 2nd sentence of the Final Privacy Rule – Regulation Text

Compliance Monitoring

- Centers for Medicare and Medicaid Services (CMS) monitors compliance on the transaction and code set standards
- The Office for Civil Rights will monitor compliance on the privacy and security regulations
- Audits can be unannounced
- The patient/customer

Compliance For Providers Means What?

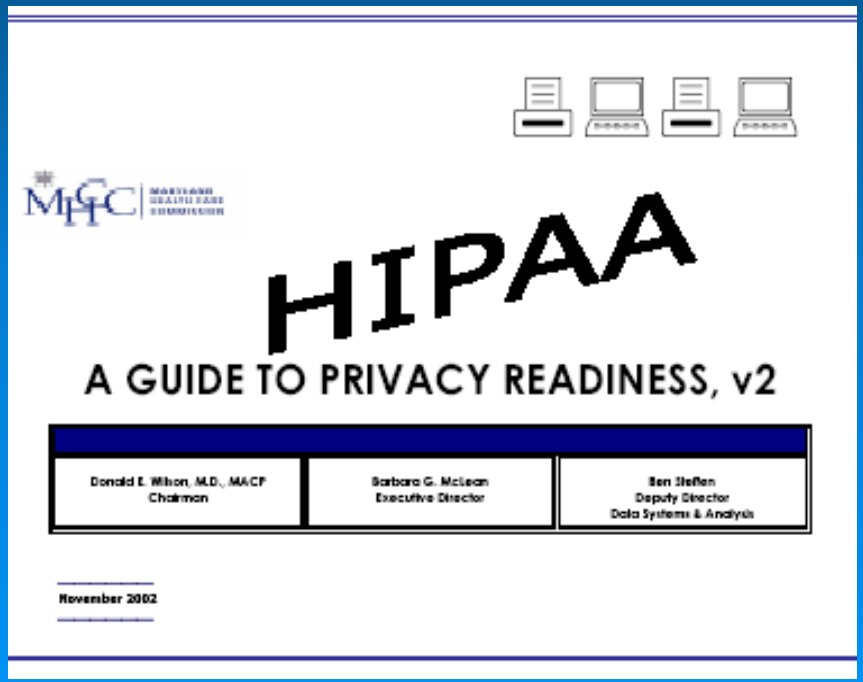
- Transaction Standards
  - Vendor self-certification letter or third party certification (include specific transactions)
- Privacy
  - Gap assessment: Q&A
  - Policies and procedures
  - Sample forms
  - Training log
- Security
  - Gap assessment: Q&A
  - Policies and procedures
  - Sample forms
  - Training log
- Ongoing review of your compliance manual is required

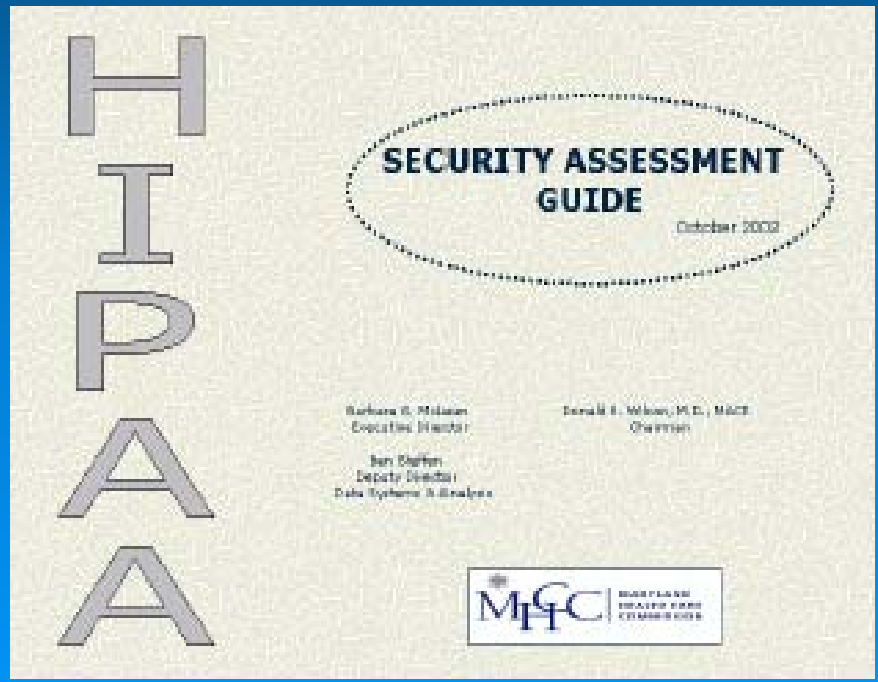
HIPAA Compliance Tools

:

Both are available at the MHCC Web-site:

WWW.MHCC.State.MD.US





MHCC HIPAA Tools: What You Can Expect To Find

Privacy tool contents:

- Introduction
- Maryland Law on the Confidentiality of Medical Records
- HIPAA Definitions
- Assessment Guide and Work Plan
- Business Associate Contract (illustrative document)
- Chain of Trust Partner Agreement (illustrative document)
- Notice of Privacy Practices (illustrative document)
- Computer and Information Usage Agreement (illustrative document)

Security tool contents:

- Introduction
- Definitions
- Small Provider Implementation Example
- Assessment Guide and Work Plan
- Administrative Procedure Checklist
- Physical Safeguards Procedures Checklist
- Technical Security Services Procedures Checklist
- Technical Security Mechanisms Procedures Checklist

Educating Patients on HIPAA--- New Role For Providers

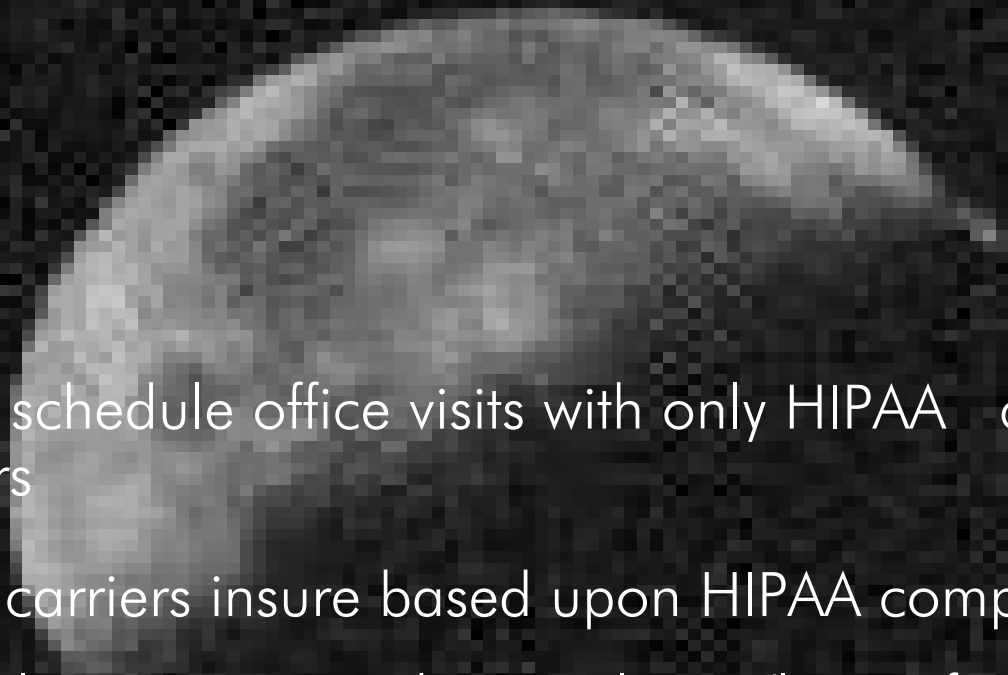
Patient Awareness Of New HIPAA Rights - Not Too Far Off...

- Right to inspect and copy protected health information
- Right to amend
- All approve uses and disclosures
- Right to an accounting of disclosures
- Right to have reasonable requests for confidential communication accommodated
- Right to file a written complaint
- Right to receive written notice of information practices

Providers Worry…

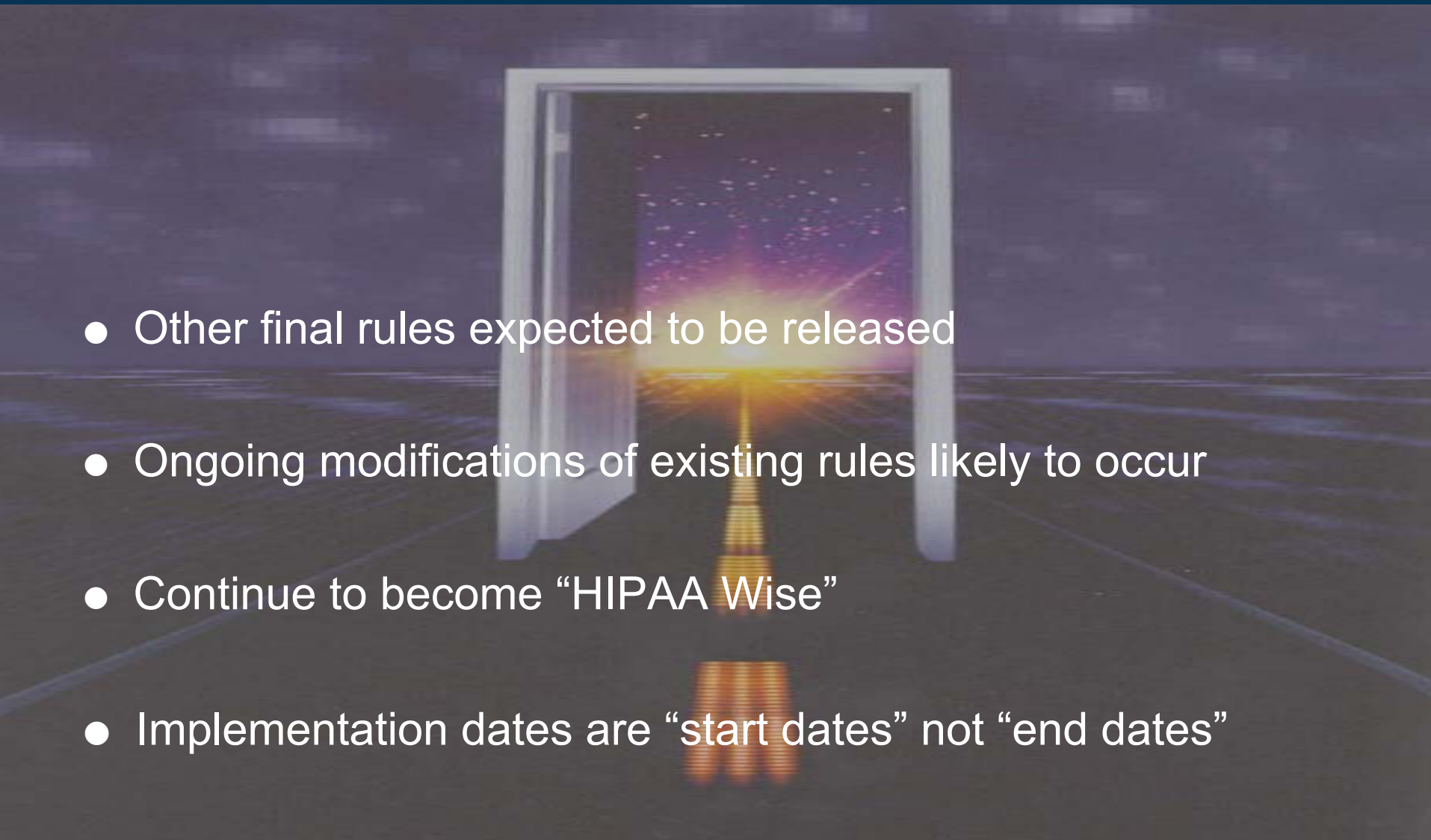
- Charts on exam room doors
- Charging patients for a copy of their medical record
- Leaving appointment reminders on answering machines
- Managing the use of temporary office staff
- Leaving medical charts in physicians offices
- Work that's defined as "in progress"

Imagine A Time Period When…



- Patients schedule office visits with only HIPAA compliant providers
- Liability carriers insure based upon HIPAA compliance
- Financial institutions underwrite loans/lines of credit based upon HIPAA compliance
- Payers request nearly all claims electronically

Lasting Thoughts…



- Other final rules expected to be released
- Ongoing modifications of existing rules likely to occur
- Continue to become “HIPAA Wise”
- Implementation dates are “start dates” not “end dates”

For More Information on HIPAA

Government sites:

http://aspe.hhs.gov/admnsimp - Department of Health and Human Services
http://www.hcfa.gov/security/isecplcy.htm- HCFA Internet Security Policy
http://www.wpc-wdi.com/hipaa -- Implementation Guides

Non-govt sites:

http://www.wedi.org
http://www.nchica.org
http://www.hipaadvisory.com/

MHCC site:
http://www.mhcc.state.md.us

MHCC | MARYLAND HEALTH CARE COMMISSION