HIPAA Training and Risk Assessment

NCMIC

Ask Mario

Mind expansion in process...

with Mario Fucinari DC, CPCO, CPPM, CIC
www.Askmario.com

1

1

The information contained in this seminar slideshow is for educational purposes and is not intended to be legal advice.

The laws, rules and regulations regarding the establishment and operation of a healthcare facility vary greatly from state to state and are constantly changing. Dr. Mario Fucinari does not engage in providing legal services. If legal services are required, the services of a healthcare attorney should be attained. The information in these seminar slides is for educational purposes only and should not be construed as written policy for any federal agency.

2

2

This presentation is sponsored by NCMIC; however, all statements and opinions expressed are those of my own and not those of NCMIC

Please note that I have authored the following books:

- *Compliance Program Manual for the Chiropractic Office*
- *HIPAA For the Chiropractic Profession*
- *E/M Guidelines for the Chiropractic Office*
- *ICD-10 Coding of the Top 100 Conditions for the Chiropractic Office*

This represents a financial interest in the product. **If you would like more information, please go to the www.Askmario.com or see me after class for more information about these products or services.**

NCMIC is not affiliated with and does not endorse any third-party products or services that may be mentioned in this presentation.

3

About Dr. Mario Fucinari, DC, CPCO, CPPM, CIC

- President, Ask Mario DC Consultants, LLC
- Certified Professional Compliance Officer (CPCO)
- Certified Physician Practice Manager (CPPM)
- Certified Insurance Consultant (CIC)
- Post-Graduate Faculty, Palmer College of Chiropractic, Logan College, Northeast College of Health Sciences (NYCC), Life West, NUHS, D'Youville College, Logan College, and Northwestern Chiropractic College
- Member, Medicare Carrier Advisory Committee
- National Speaker's Bureau for NCMIC, ChiroHealthUSA, and Foot Levelers
- Past Recipient Chiropractor of the Year

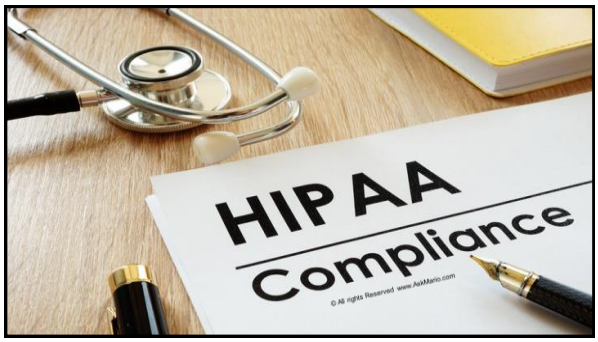
4

4

- Follow Dr. Fucinari on facebook for the latest in compliance, coding and Medicare.
- Be a friend. "Like" us at **facebook.com/askmario**
- Put us in your notifications

5

5



6

HIPAA Rules

- Congress gave us the law
- HHS gave us Privacy Rules (April 15, 2003) and Security Rules (April 20, 2005).
- Establishes officers
  - **Privacy Officer**
  - **Security Officer**
  - **Complaint Officer**

7

RISK ASSESSMENT

"The most appropriate means of compliance for any covered entity can only be determined by that entity assessing its own risks and deciding upon the measures that would mitigate those risks"

-Department of Health and Human Services

8

Required Compliance Documents

- **Corporate Compliance Manual**
  - Policies and Procedures
  - Non-Retaliation Policy
  - Non-Harassment Policy
  - Staff Training Required
- **HIPAA Manual**
  - Privacy Policy
  - Business Associate Agreement
  - Staff Training Required

LIVING DOCUMENTS
www.AskMario.com

9

Compliance Training

- ***ALL*** members of your office are to be trained on the HIPAA, Corporate Compliance, and Cures Act compliance rules.
- This includes admin, doctor(s), staff, volunteers and others who come in contact with patient information
- If you hire someone new, then they must be trained within a *reasonable* time after being hired.

10

Compliance Training

Required Compliance Training Documentation:

- Training source
- Date of training
- Notes of training
- Attendees' names must be filed with the Compliance Officer and in the employment file for each person.
- Document your policies and procedures.
  - Customize your policies and procedures
  - Be specific in documentation of the policy and the procedure

11

HIPAA Documentation Requirements

- HIPAA Manual of Policies, Procedures and Training
- Must be available for inspection
- All documentation pertaining to HIPAA **must be kept on file for 6 years**, since the *last* date of entry.
- Training of *all* personnel at least once per year

www.Askmario.com

12

13

HIPAA Privacy Rule

- The Privacy Rule establishes standards to protect an individual's medical records and other protected health information (PHI). It concerns the uses and disclosures of PHI and defines the right for individuals to understand, access, and regulate how their medical information is used.
- The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who require health care services.

14

HIPAA – Privacy Policy- General Rule (164.502)

A **covered entity** may not use or disclose protected health information except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

15

HIPAA – Privacy Policy- General Rule (164.502)

A covered entity may not **use** or **disclose** protected health information except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

16

Uses and Disclosures (160.103)

- **Uses** – information shared within the covered entity.
- **Disclosures** – sending information outside of the entity
- A covered entity may use/disclose PHI to carry out essential health care functions for TPO
  - **T**reatment
  - **P**ayment
  - Health Care **O**perations

17

HIPAA COMPLIANCE P&P

- Patient Emergency Contact Information
  - –Update at least annually
- Alternate Contacts obtained?
- Any Voice Mail Restrictions?
- Permission to text obtained?

18

In case of emergency, who may we contact or release information to on your behalf? Do you give permission to the doctor or staff to discuss your medical condition and information about your care with any family members or friends? If yes, please provide names and contact information below.

NAME	RELATIONSHIP	TELEPHONE NUMBER

19

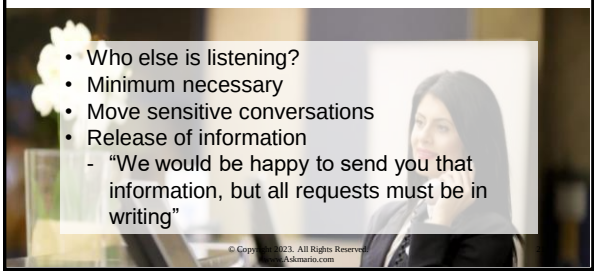
19

HIPAA Considerations Checking In

20

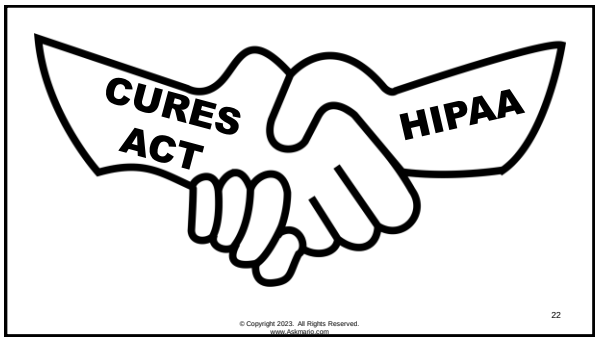
20

HIPAA Telephone Considerations



- Who else is listening?
- Minimum necessary
- Move sensitive conversations
- Release of information
  - "We would be happy to send you that information, but all requests must be in writing"

21



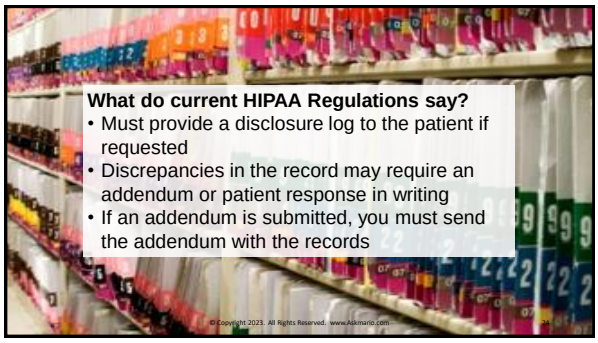
22

22

Formulate policies and procedures establishing how a patient may be granted access to their records.

23

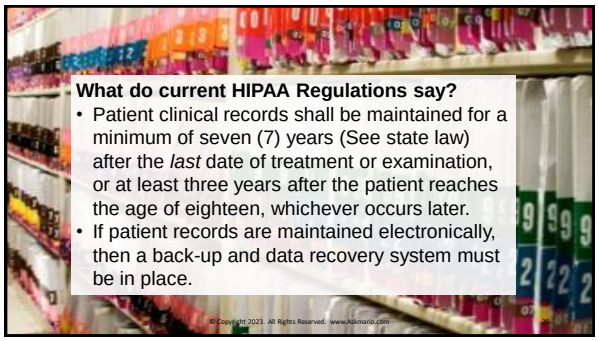
23



What do current HIPAA Regulations say?

- Must provide a disclosure log to the patient if requested
- Discrepancies in the record may require an addendum or patient response in writing
- If an addendum is submitted, you must send the addendum with the records

24



25

26

Information Blocking

Cures defines information blocking as business, technical, and organizational policies that prevent or materially discourage the access, exchange, or use of electronic health information (EHI) when an actor knows, or should know, that these practices are likely to interfere with access.

45 CFR § 171.101-103

27

"The rule includes a provision requiring that patients can electronically access all of the electronic health information, structured and/or unstructured, at NO COST."

www.healthit.gov/curesrule/

 28

28

- Health care organizations must give patients unfettered access to their full health records in digital format.
- Proposed HIPAA changes shorten the required timeframe for responding to patient record requests from 30 days to no later than **15 days.**

 29

29

HIPAA Proposed Changes:

- Strengthening patients' right to inspect their PHI in person and capture images of their PHI
- Reducing the identify verification burden on patients exercising their access rights
- Creating a new pathway for patients to direct the sharing of PHI in an Electronic Health Record among different healthcare providers and health plans

 30

30

CONTENT AND MANNER EXCEPTION

A practitioner may limit the **content** of its response to a request for electronic health record or the **manner** in which the provider fulfills the request.

45 CFR § 171.301.

31

CONTENT AND MANNER EXCEPTION

- **Manner Condition** – Establishes the *manner* in which an actor must fulfill a request to access, exchange, or use EHI in order to satisfy this exception.
- **Content Condition** – Establishes the *content* an actor must provide in response to a request to access, exchange, or use EHI in order to satisfy the exception.

EACH REQUEST MUST BE REVIEWED IN ITS ENTIRETY TO FULFILL THE REQUEST.

32

PREVENTING HARM EXCEPTION

Content: A practitioner may deny access of a patient record when the practitioner reasonably believes not providing the record is reasonable and necessary to prevent harm to a patient.

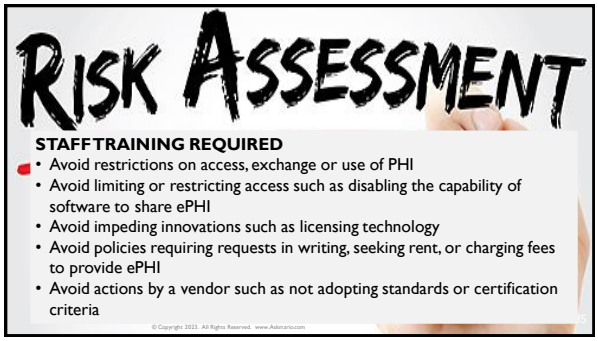
33

PREVENTING HARM EXCEPTION

Type of harm must be one that would allow a covered entity to deny access under certain HIPAA provisions, i.e.:

- Patient requests info but the licensed provider determines that access is reasonably **likely to endanger the life or physical safety of the patient** or another person (see 45 CFR 164.524(a)(3)(i)). ex. **LGBQT see state law.**
- Patient or legal rep request info but info refers to another person (other than a provider) and a licensed provider determines that access is reasonably likely to cause substantial harm to such other person (see 45 CFR 164.524(a)(3)(ii)).
- Legal rep requests info but licensed provider determines access is likely to cause substantial harm to the patient or another person (see 45 CFR 164.524(a)(3)(iii)).
- Other legally permissible access but licensed provider determines that access is reasonably likely to endanger the life or physical safety of the patient or another person (see 45 CFR 164.524(a)(3)(i)).

34



35

36

HIPAA – Privacy Policy- General Rule (164.502)

A covered entity may not use or disclose **protected health information** except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

37

Protected Health Information (PHI)

- Name
- Address
- Social Security number
- Telephone number
- Credit card information
- Photographs of an individual
- DNA samples
- Medical records
- PHI is protected for decedents also.

38

HIPAA – Privacy Policy- General Rule (164.502)

A covered entity may not use or disclose protected health information **except as permitted** or **required** by this subpart or by subpart C of part 160 of this subchapter.

39

40

HIPAA and Mental Health

- The Privacy Rule defines psychotherapy notes as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record.

41

41

HIPAA and Mental Health

- Psychotherapy notes contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for treatment, payment, or health care operations purposes, other than by the mental health professional who created the notes.
- **Therefore, with few exceptions, the Privacy Rule requires a covered entity to obtain a patient's authorization prior to a disclosure of psychotherapy notes for *any* reason, including a disclosure for treatment purposes to a health care provider other than the originator of the notes.**
- A notable exception exists for disclosures required by other law, such as for mandatory reporting of abuse, and mandatory "duty to warn" situations regarding threats of serious and imminent harm made by the patient (State laws vary as to whether such a warning is mandatory or permissible).

42

42

HIPAA and Mental Health

Does a parent have a right to receive a copy of psychotherapy notes about a child's mental health treatment?

- No. The Privacy Rule distinguishes between mental health information in a mental health professional's **private** notes and that contained in the medical record. It does not provide a right of access to psychotherapy notes, which the Privacy Rule defines as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record. See 45 CFR 164.501.
- Psychotherapy notes are primarily for personal use by the treating professional and generally are not disclosed for other purposes.

43

43

The HIPAA Privacy Notice

HIPPA PRIVACY POLICY

NOTICE OF PRIVACY PRACTICES
THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THAT INFORMATION

PLEASE REVIEW THIS NOTICE CAREFULLY.

This Practice is committed to maintaining the privacy of your protected health information ("PHI"), which includes information about your health condition and the care and treatment you receive from the Practice. The creation of a record detailing the care and services you receive helps this office to provide you with quality health care. This Notice details how your PHI may be used and disclosed to third parties. This Notice also details your rights regarding your PHI. The privacy of PHI in patient files will be protected when the files are taken to and from the Practice by placing the files in a box or brief case and kept within the custody of a doctor or employee of the Practice authorized to remove the files from the Practice's office. It may be necessary to take patient files to a facility where a patient is confined or to a patient's home where the patient is to be examined or treated. If you have further questions, please contact Mario Fuciarati D.C.

NO CONSENT REQUIRED

The Practice may use and/or disclose your PHI for the purposes of:

(a) Treatment - In order to provide you with the health care you require, the Practice will provide your PHI to those health care professionals, whether on the Practice's staff or not, directly involved in your care so that they may understand your health condition and needs.

44

44

Required Elements of the Privacy Notice

b. Header - Must use the specific language in the header as provided by the law.

   "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully."

c. Uses and Disclosures – Describe all the uses of the information for which you are not required to have an authorization.

45

45

The Provision of the Privacy Notice

- The notice must be posted "**in a prominent location**."
- The notice *must* be posted on your web site.
- The covered entity must provide a notice upon the request from *any* person.
- The patient will sign an acknowledgment that they were offered the privacy policy to read.
- If the acknowledgment is not signed, you must document why the acknowledgement was not obtained.

HIPAA Privacy Notice Acknowledgement

- The provider does not have to have a privacy policy signed prior to rendering treatment to release PHI for TPO, but the provider must make a "good faith effort" to have an acknowledgement ***on file*** that the patient has been made aware of the privacy policies.
- Answer questions for the patient.
- The patient can restrict the policies however, if the covered entity does not agree with the restrictions, treatment may be refused.

HIPAA Notice Acknowledgement

HIPAA Acknowledgement of Receipt of Notice of Privacy Practices

This authorization is prepared according to the requirements of the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), 42 U.S.C. Section 1320d, et. seq. and regulations thereunder, as amended from time to time (collectively referred to as "HIPAA"). This authorization affects your rights in the privacy of your personal healthcare information.

By signing this authorization, you acknowledge and agree that this Chiropractic ("Practice") or its Business Associates may use or disclose your Protective Health Information (PHI) to provide treatment, for purposes of relating to the payment of services rendered, and for the Practice's healthcare operations purposes.

Further, by signing this authorization, you acknowledge that you have been provided a copy of and have read and understood this Chiropractor's Privacy Notice containing a complete description of your rights and the permitted uses and disclosures under HIPAA. While this office has reserved the right to change the terms of its Privacy Notice, copies of the Privacy Notice as amended are available and can be received by sending a written request with the return address to the center where you were seen.

By signing below, you are acknowledging that you have received, reviewed, understand and agree to the Notice of Privacy Practices of this Chiropractic office, which describes the Practice's policies and procedures regarding the use and disclosure of any of your Personal Health Information created, received, or maintained by the Practice.

Acknowledged and agreed to by:

The HIPAA Fax Cover Sheet

A healthcare provider can implement the following measures:

- Store fax machines used for transmitting and receiving PHI in areas that are not accessible to the general public.
- Verify the fax number to which the documents are being sent.
- Notify the fax recipient that you are about to send a fax transmission containing confidential PHI.
- Print out a delivery confirmation report for the message you have faxed.

49

The HIPAA Fax Disclaimer

IMPORTANT: This transmission contains confidential information, which may be protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. This transmission is intended for the exclusive use of the individual or entity to whom it is addressed and may contain information that is proprietary, privileged, confidential, and/or exempt from disclosure under applicable law. If you are not the intended recipient , you are hereby notified that any disclosure, dissemination, distribution or copying of this information is strictly prohibited and may be subject to legal restriction or sanction. Please notify the sender by telephone XXX-XXX-XXXX to arrange the return or destruction of the information and all copies.

50

51

HIPAA Security Rule

- The Security Rule addresses the technical and non-technical safeguards that organizations must put in place to secure individuals' **electronic PHI (ePHI).** The Security Rule protects any data a covered entity creates, receives, maintains, or transmits in *electronic form*.
- HIPAA was established to help address the increased risks that arose when the healthcare industry began to move away from paper processes and relied more heavily on electronic information systems to conduct administrative and clinically based functions.

52

52

Ransomware Risk Analysis

- Where is your vulnerability?
  - Networks, systems, or applications
- Sources of ransomware
  - Phishing emails
  - Drive-by downloading – user unknowingly visits an infected website and malware is unknowingly installed
  - Facebook

53

53

Ransomware Policies and Procedures:

1. Set your operating system and antivirus software for automatic updates
2. Note, learn and train staff about how Ransomware originates
3. **No Facebook on office computers**
4. If an incident occurs, immediately disconnect from the network, put your device in airplane mode, turn off wifi and Bluetooth, reboot to safe mode, and alert the clinic director. Scan system for the malware, restore the computer to previous state, then report all incidents to the Curis Compliance Officer
5. Determine how the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited).
6. Document everything

54

54

Security Risk Analysis (SRA)

- All HIPAA covered entities and business associates are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by their organization.
- Download the HHS SRA Tool to help with this foundational element upon which the security activities necessary to protect ePHI are built.

55

55

Security Risk Analysis (SRA)

- Download the Windows version of the tool at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

NEW

Required: The downloadable SRA Tool is a desktop application that walks users through the security risk assessment process using multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

56

56

Do NOT give medical advice or acknowledge treatment information on social media

57

57

HIPAA Strategies

- Substitutions
  - @ for the letter a
  - $ for the letter s
  - 0 for an o
  - 3 for e

P@$$w0rd

 58

58

PHYSICAL SAFEGUARDS

 59

59

Physical Safeguards

Examples of physical security controls

- Privacy screens
- Cable locks
- Port locks
- Are cameras used?
- Alarm system

 60

60

PHYSICAL SAFEGUARD REQUIREMENTS

Disposal (R)

"Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored."

Policy: All the computers containing ePHI must be destroyed when they are no longer needed.

61

61

PHYSICAL SAFEGUARD REQUIREMENTS

"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

Policy: Create an inventory of all hardware and electronic media containing ePHI, including mobile devices such as laptops, Ipad and cell phones.

Procedure: Keep a list of all equipment. Consider engraving your office name and telephone number on computers.

62

62

TECHNICAL SAFEGUARD REQUIREMENTS

Emergency Access Procedure (R)

"Establish procedures for obtaining necessary electronic PHI during an emergency." (Disaster recovery)

- Uninterruptible power supplies
- Backup batteries and/or generators
- Offsite failover facilities

63

63

TECHNICAL SAFEGUARD REQUIREMENTS

164.312(e)(1) Transmission Security

"Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network."

– Secure Wi-Fi with password in office

64

64

What is a Business Associate?

65

65

Business Associates

A business associate is an independent contractor (not an employee) that creates, receives, maintains or transmits PHI for a function or activity regulated by HIPAA on behalf of a covered entity or even another BA.

66

66

Business Associates

- You must have an updated Business Associate agreement that outlines what to do in case of a breach. There is a decision tree that must be followed to determine the extent of the breach, if it has to be reported and to whom.
- No more than 60 days following the breach

67

67

Disposal of PHI

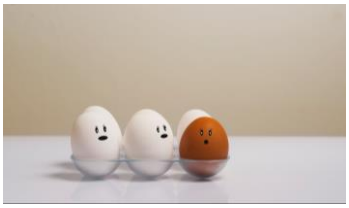
- Covered entities are not permitted to abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons.

68

68

Discrimination Awareness

69



Discrimination

Title VI of the Civil Rights Act of 1964

Federal law specifically protects individuals from many forms of discrimination in the provision of health care services. For example, those who qualify for federal health insurance programs may not be the subject of discrimination based on **gender, race, or national origin**.

70

70

Age Discrimination and Health Care

With the enactment of the Age Discrimination Act (ADA) of 1975, the federal government prohibited **age-related discrimination** by health care providers receiving funds from the DHHS. The ADA covers people of all ages.

71

71

Section 1557 of PPACA

- Section 1557 is intended to promote equity in health care and prevent discrimination on the basis of **race, color, national origin, religion, sex, age, or disability** in health programs or activities that receive federal financial assistance.
- Compliance requires posting certain notices in your office and there are consequences for failure to do so if you are not exempt.

72

72

Section 1557 of PPACA

Section 1557 Requirements are as follows:

- Having a Section 1557 compliance coordinator;
- Having a Section 1557 grievance process;
- Posting new notices - in your building, on your website and in certain publications/communications - on nondiscrimination, available assistance and patient rights;
- Posting taglines - in your building, on your website and in certain publications/communications - on the availability of language services in the top 2 non-English languages spoken in your state;
- Treating patients in a manner consistent with their gender identity;
- Not denying care to a patient based on sex, which includes their gender identity and sex stereotyping; and
- Providing equal access to communications and electronic and information technology for individuals with disabilities.

73

73

Discrimination Based on Sex

Section 1557 of the ACA makes it clear that sex discrimination is prohibited. This includes discrimination based on:

- An individual's sex or sexual orientation
- Pregnancy, childbirth and related medical conditions

Protections against Sex Discrimination

- Individuals cannot be denied health care or health coverage based on their sex.
- Women must be treated equally with men in the health care they receive and the insurance they obtain.
- Sex-specific health programs or activities are permissible only if the entity can demonstrate an exceedingly persuasive justification.

74

74

Discrimination Based on Disability

- Section 1557 of the ACA ensures that an individual is not excluded from participating in, denied benefits because of, or subjected to discrimination as prohibited under Section 504 of the Rehabilitation Act of 1973 (disability),

75

75

Discrimination Based on Age

OCR enforces the Age Discrimination Act of 1975 (Age Act), which prohibits discrimination on the basis of age in HHS-funded programs and activities.

- Under the Age Act, recipients may not exclude, deny, or limit services to, or otherwise discriminate against, persons on the basis of age.

76

76

Non-Discrimination Notice

Our office does not exclude, deny benefits to, or otherwise discriminate against any person on the basis of race, color, national origin, disability, sex, or age in admission to, or receipt of the services and benefits.

77

77

Posting of Notices in the Office

- HIPAA Privacy Notice
- Non-Discrimination Notice
- No Surprises Act Notice
- License

 78

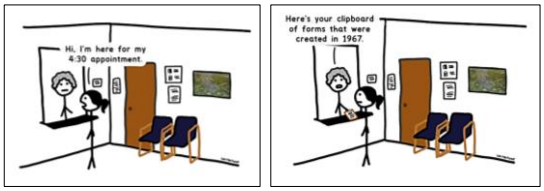
78

The “Reception Room” Décor

79

79

The “Reception Room” Décor



80

80

Intake Form Assessment

Date:_____Name:_____

Permanent Address: _____

City:_____State:_____Zip:_____

Phone: Home:_____Cell:_____Work:_____

Sex: M F SS#_____E-mail:_____

Marital Status: S M W D # of Children:_____Spouse Name:_____

Your Employer:_____Occupation:_____

How did you find out about our office? _____

(If referred by someone, please give us their name so we can thank them!)

Who is your Primary M.D.?_____Phone # _____

Emergency Contact Name:_____Phone #_____

***Please indicate how you would prefer to be reached for appointment reminders:**

_____*Text message 1 to 2 days prior to my appointment: Cell phone provider*

_____*Email 1 to 2 days prior to my appointment*

81

81

Intake Form Assessment

Date:_____Name:_____

Permanent Address: _____

City:_____State:_____Zip:_____

Phone: Home:_____Cell:_____Work:_____

Birth Date:_____Sex: M F SS#_____E-mail:_____

Marital Status: S M W D Spouse Name:_____

Your Employer:_____Occupation:_____

How did you find out about our office?_____

(If referred by someone, please give us their name so we can thank them!)

Who is your Primary M.D.?_____Phone # _____

Emergency Contact Name:_____Phone #_____

Please indicate how you would prefer to be reached for appointment reminders:

_____*Text message 1 to 2 days prior to my appointment: Cell phone provider*

_____*Email 1 to 2 days prior to my appointment*

 82

82

Intake Form Assessment

Date:_____Name:_____

Permanent Address: _____

City:_____State:_____Zip:_____

Phone: Home:_____Cell:_____Work:_____

Birth Date:_____Sex: M F SS#_____E-mail:_____

Marital Status: S M W D Spouse Name:_____

Your Employer:_____Occupation:_____

How did you find out about our office?_____

(If referred by someone, please give us their name so we can thank them!)

Who is your Primary M.D.?_____Phone # _____

Emergency Contact Name:_____Phone #_____

Please indicate how you would prefer to be reached for appointment reminders:

_____*Text message 1 to 2 days prior to my appointment: Cell phone provider*

_____*Email 1 to 2 days prior to my appointment*

 83

83

Patient Photography

- Why?
- In Office Notices
- Marketing
- Children

84

Office Photography

Formulate a policy to *not* allow photography in the office

85

Open Adjusting and The Therapy Bay

86

If you have questions…

- www.NCMIC.com
- www.AskMario.com
- Compliance and HIPAA Manuals at Askmario.com
- E-mail: Doc@AskMario.com

AskMario

87

87