MAYO CLINIC

Privacy & Security Standards to Protect Patient Information

Health Insurance Portability & Accountability Act (HIPAA)

12/16/10

Topics

- **An Introduction to HIPAA**
- **Patient Rights**
- **Routine Use of Patient Information**
- **Disclosure of Patient Information**
- **Basic Security Requirements**
- **Conclusion**

What is HIPAA?

Health **I**nsurance **P**ortability and **A**ccountability **A**ct

HIPAA is a federal law.

The Department of Health & Human Services issued HIPAA privacy standards and security standards to protect patient information from inappropriate use or disclosure.

HIPAA regulations apply to all Mayo Clinic entities – Rochester, Arizona, Jacksonville, Mayo Health Systems.

Health Insurance Portability and Accountability Act (HIPAA)

What does HIPAA mean to YOU?

Our patients trust us to protect their privacy and keep their information confidential.

Mayo's commitment to preserving that trust and protecting all of our patients privacy has not changed. It has only been reinforced by the HIPAA standards.

ALL of our patients are protected by HIPAA.

What are the HIPAA Requirements?

HIPAA standards require the following:

1. Inform patients that they have rights, such as the right to obtain copies of most of their health information and the right to request amendments.

2. Inform patients how their health information may be used and disclosed.

3. Verify that those to whom we give patients' health information (e.g. business associates) also maintain its confidentiality.

4. Meet administrative requirements, such as appointing a Privacy Officer at each site and documenting how we interact with patients about their rights.

5. Ensure that only authorized people have access to patients' information.

What information is protected by HIPAA?

HIPAA standards apply to all “protected health information” which includes demographic information and any identifying information about the patient, such as:

1. Name
2. Address
3. Dates related to the patient (e.g. birth date, appointment dates)
4. Telephone numbers, fax numbers, and e-mail addresses
5. Identifying numbers that are specific to the patient, such as social security number, medical record number.
6. Pictures of the patient

All patient information and demographic information is protected, whether it is on a computer, in a paper record, or verbal.

Topics

- An Introduction to HIPAA
- Patient Rights
- Routine Use of Patient Information
- Disclosure of Patient Information
- Basic Security Requirements
- Conclusion

Patient Rights

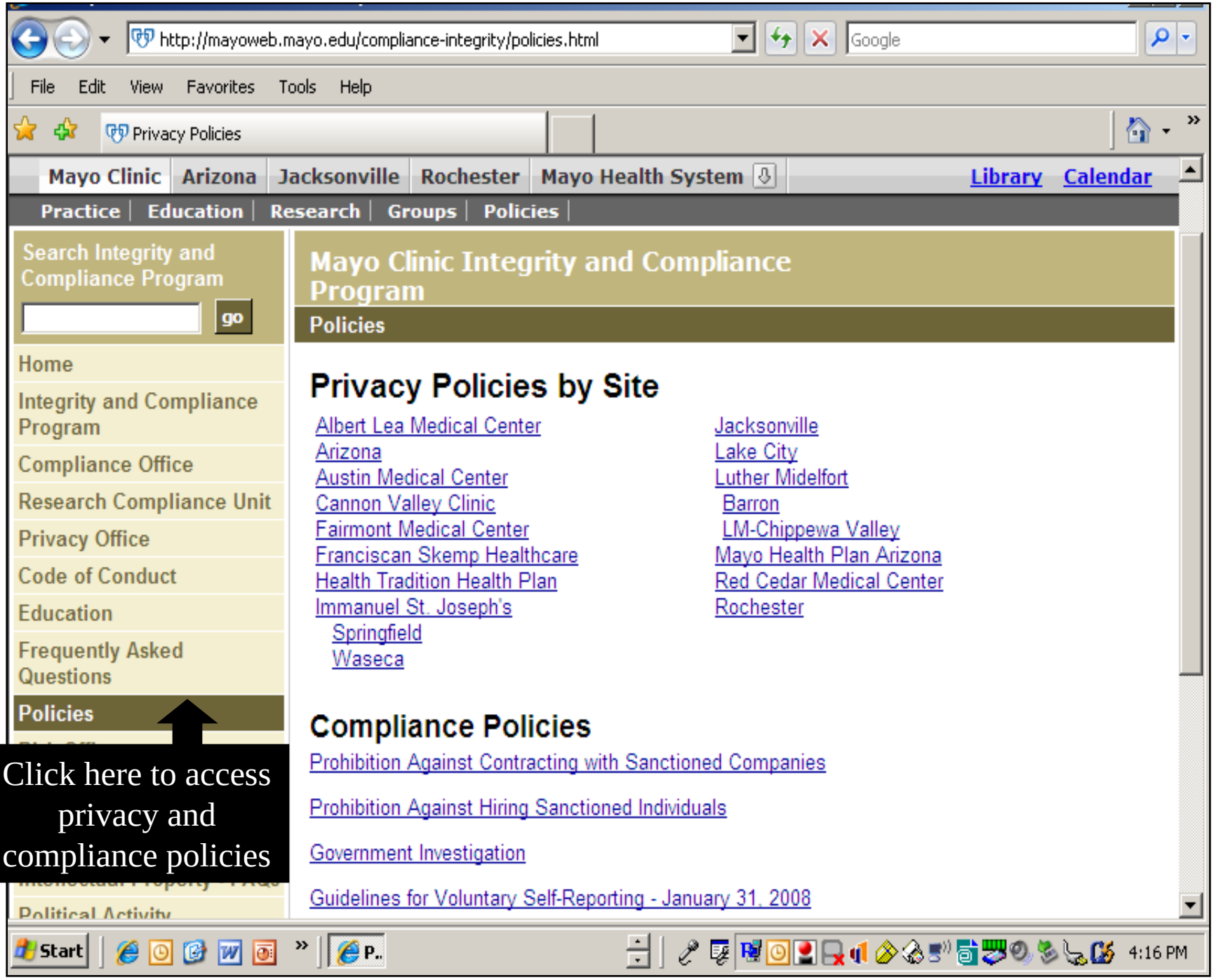
Six areas of patient rights related to health information have been mandated by HIPAA.

1

Patients have the right to see and obtain copies of their health information

Most patients can see their entire medical record. However, there are a few exceptions (e.g. if the patient is at risk of injuring him/herself), so it's important that you refer to your site's privacy policy.

Privacy policies by site are located at the Integrity & Compliance web page.


http://mayoweb.mayo.edu/compliance-integrity/policies.html
Google
File Edit View Favorites Tools Help
Privacy Policies
Mayo Clinic Arizona Jacksonville Rochester Mayo Health System
Library Calendar
Practice Education Research Groups Policies
Search Integrity and Compliance Program
go
Home
Integrity and Compliance Program
Compliance Office
Research Compliance Unit
Privacy Office
Code of Conduct
Education
Frequently Asked Questions
Policies
Mayo Clinic Integrity and Compliance Program
Policies
Privacy Policies by Site
Albert Lea Medical Center
Arizona
Austin Medical Center
Cannon Valley Clinic
Fairmont Medical Center
Franciscan Skemp Healthcare
Health Tradition Health Plan
Immanuel St. Joseph's
Springfield
Waseca
Jacksonville
Lake City
Luther Midelfort
Barron
LM-Chippewa Valley
Mayo Health Plan Arizona
Red Cedar Medical Center
Rochester
Compliance Policies
Prohibition Against Contracting with Sanctioned Companies
Prohibition Against Hiring Sanctioned Individuals
Government Investigation
Guidelines for Voluntary Self-Reporting - January 31, 2008
Click here to access privacy and compliance policies
Start
4:16 PM

2

Patients have the right to request amendments to the information in their medical record

Patients have the right to request amendments to their medical record if they believe that their record is incomplete or inaccurate.

The process varies by site, and involves active participation by the physician/provider so you must follow the privacy policies for your site if patients request amendments to their medical records.

3 Patients have the right to know about certain non-routine disclosures of their health information

Patients may request a list of non-routine disclosures of their health information. For example, when the patients PHI is disclosed to a third party or patient information released under a subpoena must be documented and included in a list that is provided to the patient upon request.

Disclosure is <u>not</u> required if:

- The information is released for patient treatment, payment for services, or healthcare operations.
- Disclosures have been specifically authorized by the patient.

Refer to your site's Privacy Policies for guidance.

<u>Important Note</u>: State law may require Mayo to follow additional guidelines. For example: Wisconsin state law requires that all disclosures of health information, with no exceptions, be documented.

4

Patients have the right to request that their health information be communicated in a certain way

Patients have the right to discuss their health information confidentiality. Don't speak to a patient in a crowded area about confidential information like why the patient is being seen at Mayo instead you should ensure you are in a isolated spot where confidentiality is easier to maintain.

Patients may also request that their health information be communicated in a specific way – as when a patient wants information sent to a different address than what is in his/her medical record. For example, a patient may not want certain laboratory test results sent to the home address.

The department communicating with the patient is responsible for handling the patient's request for confidential communications.

5

Patients have the right to request restrictions on how their health information is used or disclosed

We may use a patient's information for their treatment, payment for services, and to conduct healthcare operations.

If a patient requests a restriction on how their information is used, it is important that you refer to your site's policy in order to give patients a consistent and accurate response to their request and consult your site Privacy Officer with any questions.

6

Patients have the right to complain to us, and to the government, about our privacy practices or about a violation of those privacy practices

Keeping patient information private is a primary concern at Mayo. We take privacy and confidentiality very seriously – but mistakes sometimes happen.

If patients feel that their privacy has been violated, they have the right to complain.

Follow the guidelines in your site's policy.

Topics

- An Introduction to HIPAA
- Patient Rights
- **Routine Use of Patient Information**
- Disclosure of Patient Information
- Basic Security Requirements
- Conclusion

Routine Use of Patient Information

How is patient information protected?

Mayo has established policies governing how patient information can be used.

If you routinely handle patient information and encounter patients as part of your job, it is important that you understand how to respond in different situations so that patient confidentiality is protected.

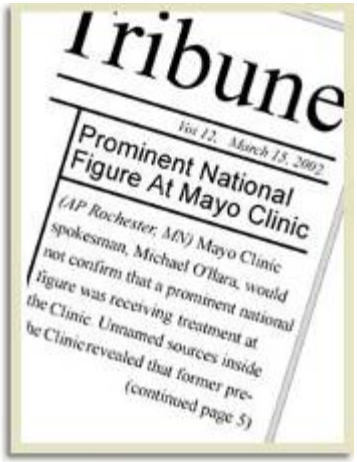
What about this . . .

Is the fact that a patient was here *<u>confidential</u>*?

<u>Yes</u>!

Individuals trust us to keep their presence – and their information – confidential.

- If you recognize a patient, keep it to yourself
- Do not talk about patients with your colleagues unless it is necessary to do so for your job
- It is inappropriate to discuss patients outside of the workplace.


Tribune

Vol 12, March 15, 2002

Prominent National Figure At Mayo Clinic

(AP Rochester, MN) Mayo Clinic spokesman, Michael O'Hara, would not confirm that a prominent national figure was receiving treatment at the Clinic. Unnamed sources inside the Clinic revealed that former pre-

(continued page 5)

Health Insurance Portability and Accountability Act (HIPAA)

Someone may be able to identify a patient based on the content of your conversation, even if you do not identify the patient by name.

For example: At a dinner party, you may talk about an extremely rare cancer that was treated with an interesting experimental surgery.

If one of the people at the dinner party knew someone with the same extremely rare cancer, your conversation may reveal details about their care. Do not place yourself, your co-workers, or your employer in a compromising situation because you fail to respect a patient's privacy.

Keep all patient information private.
It is the right thing to do. And it's the law.

What about this . . .

You overhear others talking about patients?

All patient information, *written and verbal*, is protected by HIPAA.

For example, if you overheard a physician speaking with a resident about a patient on the elevator, do not pass it on.

You could also remind them that they should protect patient confidentiality by not talking about patients in front of others not directly involved in their care.

If you need to talk about a patient, pay attention to who may overhear your conversation. Look for a private place to speak if others, especially members of the public, can hear you.

What about this . . .

You unintentionally see patient information?

As a member of our workforce, you will occasionally encounter patient information for patients not under your care. For example, you may see a patient's medical record at a nursing station.

Regardless of how it happens, you should avoid looking at patient information unless you are ***directly involved*** in that patient's treatment.

Patient information is *always* protected and must *always* remain confidential.

What about this . . .

You are concerned that others are not being careful with patient information?

This can put you in an uncomfortable situation. However, there are several actions you can take – and doing the right thing is important to protecting our patients' trust.

- Remind them of their responsibilities to keep patient information confidential.
- Talk to your supervisor.
- Call your Privacy Officer.

What about this . . .

What is your responsibility in providing a patient's information to another staff member?

- Verify the identity of anyone who requests patient information from you.
- Verify that it is necessary for the requestor to see the patient's information (is there a "need-to-know" reason?).
- Contact your Privacy Officer for additional information about verification of employee identity or authority.

How can we use patient information?

It is OK to use patient information for:

- ***Treatment:*** This includes providing, coordinating or managing healthcare and related services for a patient, which can also involve communications with other providers about patient treatment or referral of a patient to another provider.

- ***Payment:*** Activities undertaken to obtain reimbursement for healthcare services.

- ***Healthcare Operations:*** This includes quality assurance, medical review, legal services, auditing functions, and general administration.

You need written patient authorization to use patient information for purposes other than treatment, payment or healthcare operations. Check with your supervisor or Privacy Officer.

How much patient information can we use?

Your department will determine what types of patient information are required to do your job. The "need-to-know" rule is HIPAA's minimum necessary standard.

- Not every employee needs access to a patient's entire medical record.
- Clinical staff (e.g. physicians, nurses) generally need to see the whole patient record to properly care for a patient. Other staff, however, may only need the patient address and phone number for appointment scheduling.
- Clinical personnel should only access patient information when they have a treatment relationship

"Curiosity viewing" of patient records is absolutely prohibited.

Topics

- An Introduction to HIPAA
- Patient Rights
- Routine Use of Patient Information
- **Disclosure of Patient Information**
- Basic Security Requirements
- Conclusion

Disclosure of Patient Information

HIPAA requires us to obtain patient authorization for certain disclosures if it is necessary to disclose a patient's information ***outside of our organization***.

- HIPAA specifically requires patient authorizations for disclosures of ***psychotherapy notes*** and for ***marketing purposes.***
- Authorization forms have been updated to reflect the specific HIPAA requirements.

Contact your Privacy Officer if you have questions about circumstances requiring the disclosure of patient authorization

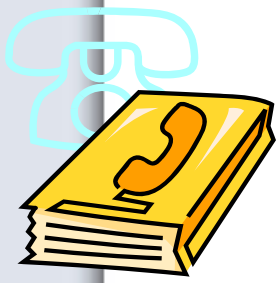
Are there limits to the amount of patient information we can disclose?

Yes

The minimum necessary standard applies to disclosures of patient information outside of our organization.

- If another provider requests information on a patient's insurance plan, we should send only the information requested and ***not*** the entire record.
- When we request patient information from others, we should ask ***only*** for information required for our purpose.

What if a patient does not want to be included in the facility directory?



The facility directory contains patient's name, location in the facility, general condition, and religious affiliation.

If a patient requests not to have this information disclosed to the public, we need to comply.

The patient’s directory information will remain available to our internal staff so that we can locate the patient.

Can patient information be released to people and organizations with whom we do business?

Yes

The HIPAA privacy rule allows us to release patient information to “business associates”, persons or organizations that receive patient information in order to perform a service or function for us. There must be a valid business associate agreement in place, however.

Can de-identified patient information be disclosed under HIPAA?

There are situations, such as lectures or publications, where de-identified patient information may be appropriately disclosed.

There are specific criteria that must be met for information to be considered “de-identified.”

Refer to your site’s policy on de-identified information or contact your privacy officer.

Topics

- An Introduction to HIPAA
- Patient Rights
- Routine Use of Patient Information
- Disclosure of Patient Information
- **Basic Security Requirements**
- Conclusion

Basic Security Requirements

Security is responsible for how information is protected.

Privacy involves how information is used and disclosed.

- Federal law requires us to have security policies and practices to protect our patients' information against unauthorized access.
- Mayo Clinic is committed to following the law and protecting their reputation for respecting patient privacy and security.
- Policies exist to ensure that all transactions are secure and protected – this includes electronic information stored on our computers and information sent via email and fax.

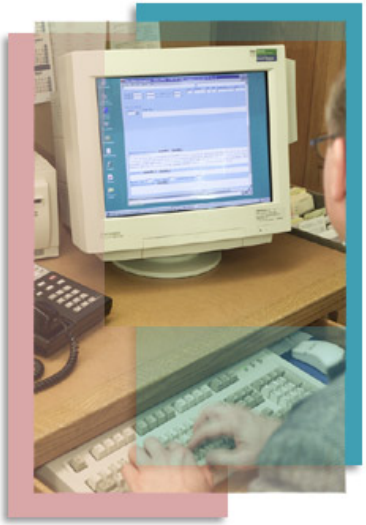
Find more information at the Mayo Clinic Security web page.

What does information security mean to you?

How do you protect your work area?

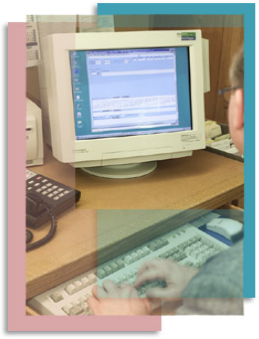
How do you protect your computer?

- Lock up or keep out of sight any confidential information to ensure that unauthorized people do not see it.
- Face your computer screen away from public view.
- Talk to your supervisor or manager if you need assistance.



Do you have a password-protected screen saver on your computer?

You should!



- Set your computer so that a screen saver engages after a short period of inactivity.
- Always remember to lock your workstation or log off when you leave your work area.
- Ensure that no one has access to your computer while you're away from you desk.

Protect your user name and password

These steps will protect you as well as our patients.

- Do not share your password with anyone.
- Do not write your password anywhere.
- Do not post your password on your computer screen.
- Do not place your password under keyboard.
- Memorize your user name and password and keep them to yourself.

You are responsible for all computer activity using your user name and password.

Password Requirements

- Change your password according to policy or anytime you feel it has been compromised.
- Use at least six characters.
- Include both letters and numbers.
- Do not use your name or others' names.
- Do not use words found in the dictionary.
- Do not use the word "password".

Protect your computer against viruses

Avoid the harm that computer viruses can cause to our computers, networks, and the information that they contain (such as losing or altering information or rendering the network unusable).

- Do not copy computer programs from Mayo to use on computers at home.
- Do not copy programs from home to load onto your work computer.
- **Do not open files or e-mail attachments unless you know and trust the source. Delete them without opening.**

Contact your local technical support for further assistance with transferring information.

Health Insurance Portability and Accountability Act (HIPAA)

If you need to transfer information from home to work or work to home:

- ✓ Run “virus check” before the information is transferred.
- ✓ Use anti-virus software on your home computer.

Using the Internet and e-mail at work

Internet and email are intended for business use.

Employees are allowed to use the Internet and e-mail for limited personal use, as long as it does not interfere with job performance or impose more than minimal demands on our electronic mail system.

- When you use the Internet and e-mail for personal purposes, it increases the risk of getting viruses from other computer systems.
- If you receive unsolicited e-mail, junk e-mail, or chain letters, be sure to delete them. ***Do not pass them on.***

Remember: E-mail is official correspondence. Do not include anything in an e-mail message that you would not be comfortable having a third party see, such as inappropriate or derogatory language**.**

Confidential Information

- ***Carrying it***
- ***Mailing it***
- ***Faxing it***
- ***Emailing it***
- ***Destroying it***

Carrying Confidential Information

- ✓ Paper documents containing confidential information should be carried in an enveloped marked “Confidential.”
- ✓ Confidential information contained on USB drives or other electronic media must be encrypted.
- ✓ Never leave items containing confidential information in your car or any unattended place where others might take it including your electronic device.

Mailing Confidential Information

- ✓ With “intraclinic” mail, you should use an envelope marked “Confidential.”
- ✓ When mailing to an external destination, you do not need a “Confidential” envelope. Use either the United States Postal Service or a special delivery service (e.g. Federal Express (FedEx) or United Parcel Service (UPS). Please ensure that the envelope is sealed.
- ✓ Magnetic media must be encrypted and may require special shipping procedures. Contact your supervisor or your mailroom or the Information Security Office.

Faxing Confidential Information

- ✓ Make sure you have the correct fax number.
- ✓ Make sure the recipient picks up the fax promptly.

Send a fax cover sheet that includes:

- ✓ A statement that the information is "Confidential." (Do not include any confidential information on cover sheet).
- ✓ A "disclaimer“ explaining that if the information was sent to the wrong place, the recipient should call you immediately and destroy the attached confidential information.

E-mailing Confidential Information

- ✓ E-mail containing confidential information must ***not*** be routinely sent outside of the Mayo organization.
- ✓ E-mail containing confidential information should contain your contact information.
- ✓ If you receive an e-mail in error, you should notify the sender and then delete the e-mail.

If you must e-mail confidential information outside the organization, please contact local technical support for a secure solution.

Destroying Confidential Information

- ✓ If electronic or magnetic media (such as floppy disks, tapes, CD-ROMs, hard drives) need to be destroyed, contact your local technical support for guidance.
- ✓ If a great deal of paper-based confidential information needs to be destroyed, contact your Privacy Officer.

Contact the Information Security Office for additional guidance and a list of frequently asked questions.

Topics

- An Introduction to HIPAA
- Patient Rights
- Routine Use of Patient Information
- Disclosure of Patient Information
- Basic Security Requirements
- Conclusion

Health Insurance Portability and Accountability Act (HIPAA)

- Do not give patient information to anyone unless there is a "need-to-know" reason for their job function.
- When you need to discuss patient information, pay attention to who may overhear your conversation. Look for a private place to speak if others may hear you.
- If you overhear others inappropriately discussing a patient, remind them that they have an obligation to maintain patient confidentiality.
- Keep patient information out of public traffic areas. For example, do not leave paper containing patient information where others can see it.
- Be responsible when disposing of protected health information.

Health Insurance Portability and Accountability Act (HIPAA)

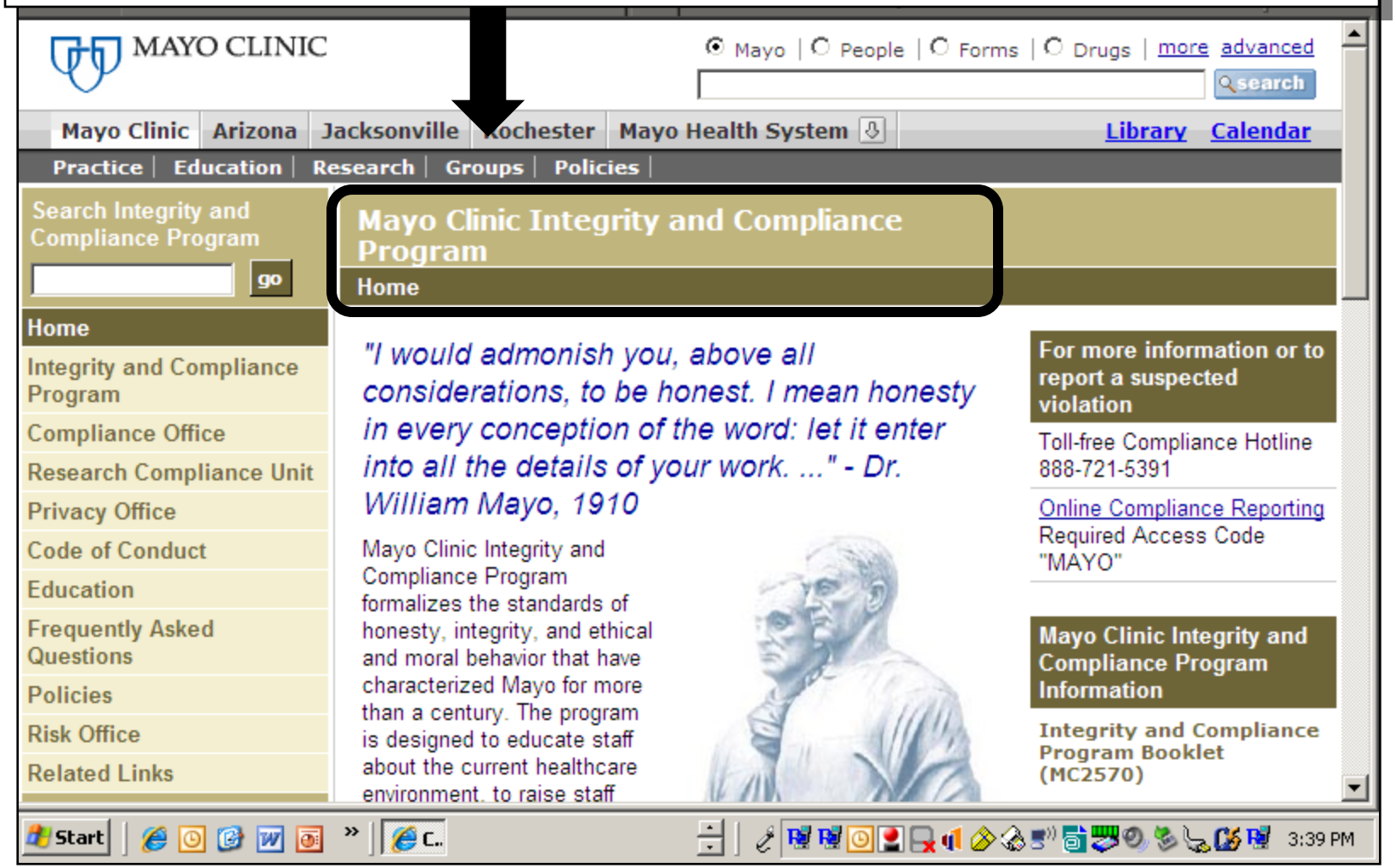
Please contact your local Privacy Officer any time you need help with any questions or concerns.

Go to the Integrity & Compliance web site for additional resources.

Remember to always follow the policies and procedures at your site on protecting the confidentiality of all protected health information including patient information.

Useful resources on the Mayo Intranet!

Under “Groups”, look for the *Compliance Office*.




http://mayoweb.mayo.edu/compliance-integrity/privacycontacts.html
Google
File Edit View Favorites Tools Help
Privacy Contacts
Search Integrity and Compliance Program
go
Home
Integrity and Compliance Program
Compliance Office
Research Compliance Unit
Privacy Office
HIPAA Background and Overview
Contacts
Tools & Resources
Related Links
Click here for the list of Privacy Officers
Mayo Clinic Integrity and Compliance Program
Privacy Contacts
Jacksonville Barbara McCarthy 3-2958 or 904-953-2958
Rochester Eric W. Klavetter 6-0195 or 507-266-0195
Arizona Deborah Jaskowski 2-6255 or 480-301-6255
MMSI Deborah A. Shirley 8-5048 or 507-538-5048
MCSI Sharon Zehe 4-2685 or 507-284-2685
Mayo Health System Administration Kay Kluge 4-0238 or 507-284-0238
Mayo Medical Transport Thomas J. Fennell 320-251-2302
Mayo Clinic Health Solutions Tracy M. Berg 8-1203 or 507-538-1203
Mayo Health System
Location Contact Phone
Albert Lea Medical Center Laure Buehrer 507-379-2018
Austin Medical Center Tammy L. Kritzer 507-434-1284
Cannon Falls Medical Center Randi J. Widstrom 507-263-7675
Start
3:46 PM

Health Insurance Portability and Accountability Act (HIPAA)

Confidentiality breaches are very serious matters. Staff who knowingly violate our policies on confidentiality will be dealt with appropriately.

To report suspected violations of Mayo's Code of Conduct or HIPAA regulations regarding patient confidentiality, you can make an anonymous, confidential report at any time.

- Call the toll-free Compliance Hotline, 1-888-721-5391
- Go online at: www.MayoClinicComplianceReport.com
  (copy and paste link to a new browser)

These are also noted on the Integrity & Compliance Home Page

You have finished the module
"Health Insurance Portability and Accountability Act (HIPAA)"

Thank you for your time.

If you would like your education transcript updated to reflect completion of this course, please contact the Compliance Office at 507-266-6286 or 507-538-3437 or email COMPLIANCEOAA@mayo.edu