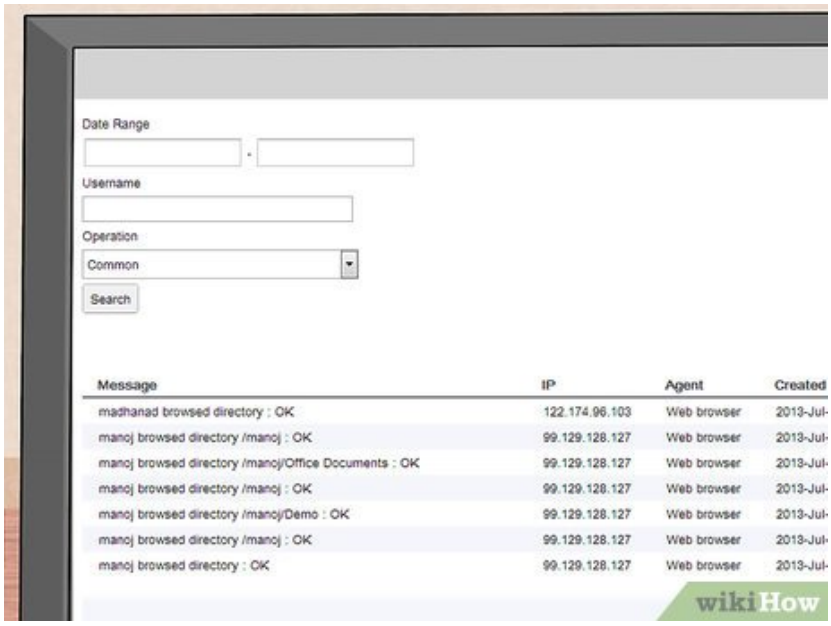
How to Make Software HIPAA Compliant

The federal government's Health Insurance Portability and Protection Act (HIPAA) created guidelines for how healthcare providers handle patient health data. Unfortunately, the HIPAA guidelines are vague. There is no easy checklist you can...

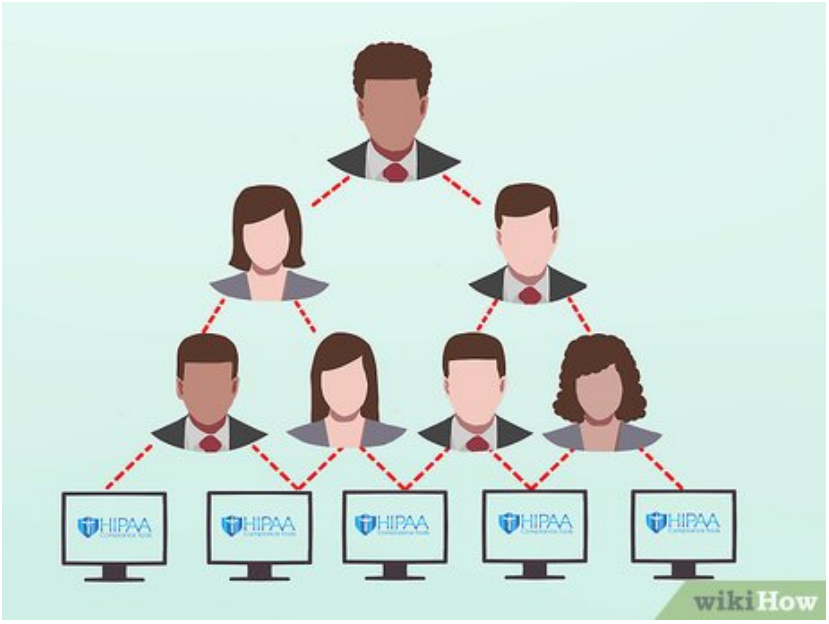
Part 1 of 3:

Creating Appropriate Procedures

1. 

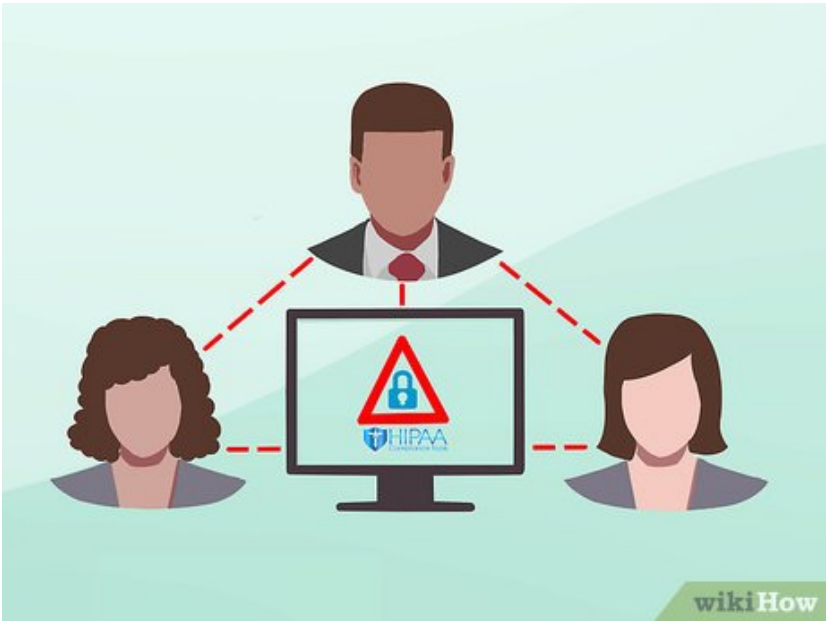
Keep an audit log. You need to track who accesses a patient's record. This means that you need to create separate usernames and passwords for each person who has access to patient health information. As part of the audit log, you should track the following:

1. which record the user accessed
2. the date it was accessed
3. whether the user viewed the information, updated it, or deleted it

2. 

Create levels of access. HIPAA also requires that an employee only see the 'minimum necessary' information to do their job. For example, a doctor will need to see more health information than a receptionist. Accordingly, you need to create levels of access, in which you provide only as much information as each person needs to do their job.

1. Some employees might only work with certain patients. In this situation, they should be granted access only to the patient records for the people they work with.
2. In order to successfully create levels of access, you need to clearly define roles in your organization. This might require that you look at job descriptions and rearrange duties.

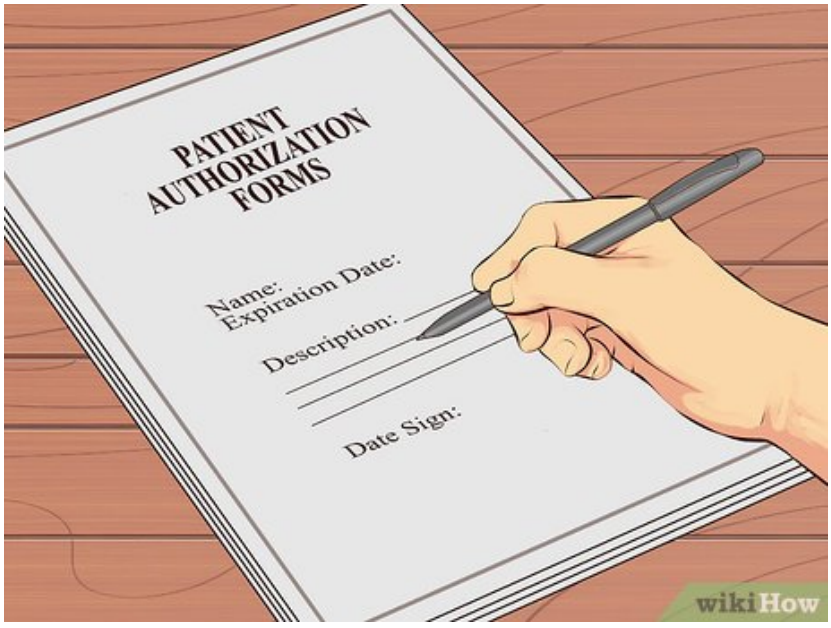
3. 

Create an 'emergency override' function. Even if you create levels of access, there may be situations where someone needs to access all information in an emergency. For this reason, you should create an 'override' which allows the person to retrieve whatever information is necessary to effectively treat patients.

1. Nevertheless, you should set up your software so that use of this override function undergoes scrutiny.
2. For example, you could set up the software so that every time someone uses the override function several other people are automatically emailed simultaneously. The software should also track whatever information this person accesses.
3. You should also write out a review process for each use of the override function. For example, the person who uses it might have to meet later with a supervisor to justify the use.
4. 

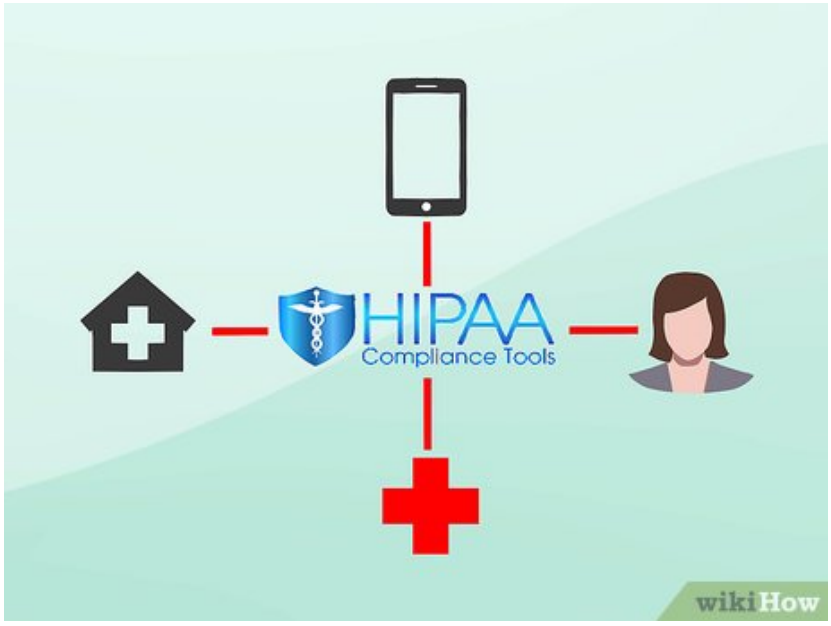
Secure your data. HIPAA requires that you keep your data secure. In practice, this means that you should use passwords and keep the data secured behind a firewall.

1. You also need to ensure that your emails are secure. In particular, you must use sufficient encryption technology on your emails.
2. For more information on making sure your email complies with HIPAA, see Make Email HIPAA Compliant.

5. 

Scan patient authorization forms. You are required to get patients to sign forms authorizing your use of their information for their care. Each form should include a description of what you will use the data for and the date of expiration.

1. You should track these authorizations, including the date the form was signed and the name of the person signing it.
2. You should also scan the form and maintain a digital copy.

6. 

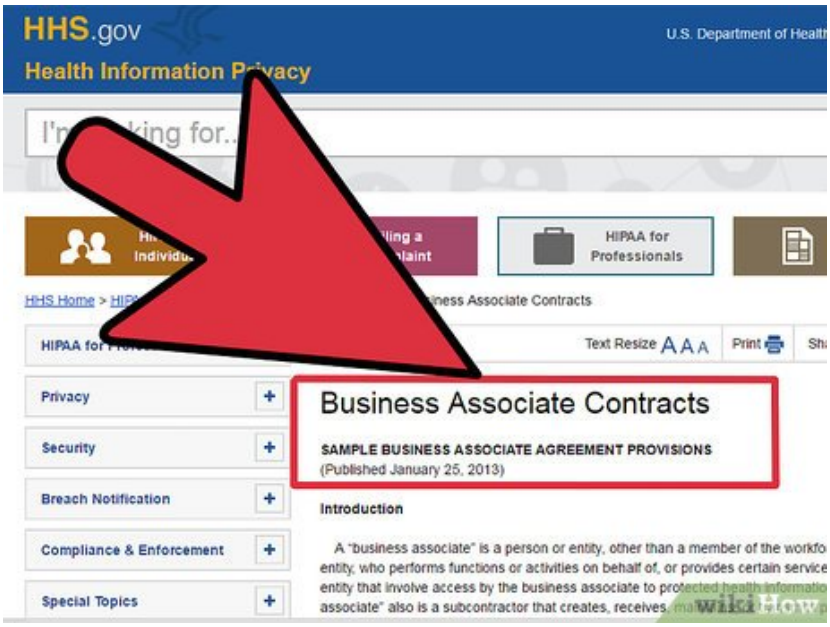
Confirm that your billing system is compliant. HIPAA standardized the transmission of billing information. For this reason, whatever billing system you use must support the HIPAA standards.

1. At this point in time, virtually every billing system on the market does. Nevertheless, you should confirm with your vendor that it is HIPAA compliant.

7. 

Ask vendors about backup. HIPAA also requires that you maintain your data so that a patient can see it whenever he or she requests it. This means that you must maintain backups of all information. If you keep information on paper, then you need copies stored off-site or digital scans created. If you store data electronically, then it must be backed up.

1. Ask vendors how they back up their systems. Find out how they ensure the continuity of the system in case of an accident.
2. Should you host the data system on your own servers, then you will need to find out what backup procedures you have in place, as well as your emergency plans.

8. 

Have business associates sign contracts. Anyone who sees your data must agree to uphold the same policies and procedures as your organization. You should therefore draft a 'Business Associate' contract for all vendors to sign.

1. Health and Human Services has a sample contract available at http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html. You can modify it to suit your purposes.
2. There are also sample contracts on the Internet. For example, the UT Health Science Center has a form contract you can use.[1]
3. You should also have your health care attorney look over any contract to make sure that it is sufficient to protect you.

Part 2 of 3:

Searching for Software and Data Vendors

1. 

Ask other health care providers. If you are opening a business, then you will need to purchase software. You also might need to hire someone to host your data on their servers (or to back up your own servers).

1. Ask other providers what vendors they use. Virtually all healthcare providers are covered by HIPAA, so they should have given considerable thought to whether or not their software is compliant. You should ask for recommendations.

2. 

Compare prices. After getting recommendations for different vendors, you need to compare their prices. You should call them to get a quote. Their phone numbers should be on the Internet.

1. Prices will depend on the number of people who need to access your system, so make sure you have that number available.[2]
2. If your business is growing, then you should think a couple years ahead. For example, if you have five employees but think you will double in size, then make sure you get a quote for how much it costs to have 10 users. You don't want to switch software after only a year.

3. 

Find out how the vendor monitors changes in HIPAA. HIPAA regulations continue to evolve. You should expect the vendor to keep up with changes in the law. When contacting vendors, you should ask the following:

1. How does the vendor monitor changes in HIPAA regulations? Does it have an action plan for keeping up with changes in the law? Look for concrete examples. Does the company have a lawyer

on staff who monitors changes in the law?
2. What percentage of the vendor's clients must be HIPAA compliant? If most of the company's clients must comply with HIPAA, then you can be sure that it will make necessary changes to comply with HIPAA—or else it will go out of business.

Part 3 of 3:

Understanding HIPAA's Requirements

1. 

Check if HIPAA applies to you. You must comply with HIPAA if your organization transmits any billing information electronically to any health insurance company, including Medicaid and Medicare. The information can include invoices or other information needed to find insurance coverage. Generally, HIPAA regulates providers of the following:

1. therapy
2. counseling
3. medical care
4. any other service which bills insurance companies

2. 

Find a health care attorney. HIPAA rules are complicated and difficult to understand. In order to make sure that you are in compliance, you should hire a health care attorney for your organization. A health care attorney can help address risk management and regulatory issues.[3] You can keep this person 'on retainer,' which means that you pay a fee each month. In exchange, the lawyer is always available to answer your questions.[4]

1. You can get recommendations for a health care lawyer by asking other health care providers who they use. If you don't get any recommendations, then you can visit your state's bar association, which should run a referral program. Ask for a referral for a health care attorney.
2. Be sure to ask the lawyer about his or her experience. You will want someone who has extensive experience in regulatory compliance, not simply in representing businesses in lawsuits.

3. 

Be safe, not sorry. Technically, you don't need to create usernames, levels of access, or even have software in your organization. Instead, HIPAA only requires that you take 'reasonable steps' and disclose

only the 'minimum necessary' information. Nevertheless, as a practical matter, you need to create the procedures for accessing and distributing information described above if you plan to run a modern office using computers and email. These procedures will help protect you from unauthorized disclosures of patient information.

1. The penalties for violating HIPAA can be severe. You can face up to a $50,000 fine for each violation, up to a maximum of $1.5 million each year. There are also criminal penalties for those who knowingly violate the rules.
2. Accordingly, you are better off following the practices and procedures which are becoming standard in your industry. Experienced health care attorneys and vendors can guide you in the right direction.