10 Most Common HIPAA Mistakes and How to Avoid Them

Compliance Helper

The 10 Most Common HIPAA Mistakes and How to Avoid Them
About HIPAA Compliance Tools

HIPAA Compliance Tools is a medical management consultant firm that has been involved with the health care industry for approximately 10 years. It has streamlined HIPAA Compliance procedures for thousands of doctors, dentists, hospitals and clinics.

HCT offers many products and programs that have assisted healthcare organizations and employers meet their compliance and operational needs. HCT has recently combined with Compliance Helper to deliver the most effective method for compliance in the industry.

Compliance Helper has teamed with Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, “The Privacy Professor”®, to build a cloud based solution for HIPAA HITECH Information Security and Privacy compliance.

Our Internet-based service delivers customizable policies and procedures built around international information security and privacy standards and mapped to HIPAA/HITECH and other regulatory requirements, forms, a step-by-step process which includes gap analysis, and an expert human helper to assist business associates and covered entities in attaining and maintaining information security and privacy compliance.

If you have questions please click here.
Contents

About HIPAA Compliance Tools ................................................................. 3
Introduction .................................................................................................. 5
Special Offer ............................................................................................... 6
Mistake 1: Not knowing what being a "covered entity" means ..................... 7
Mistake 2: Failing to Comply With the Security Rule ............................... 10
Mistake 3: Not Taking the Time to Train and Retrain Employees ............ 13
Mistake 4: Ignoring State Privacy Laws .................................................... 16
Mistake 5: Forgetting to update the notice of privacy practices and/or send the three year reminder ............................................................ 18
Mistake 6: Lacking a Written Procedure for Investigating and Resolving Privacy Complaints ................................................................. 21
Mistake 7: Not Understanding HITECH .................................................... 24
Mistake 8: Being Uninsured for HIPAA Investigations Against Business .... 27
Mistake 9: Oral Privacy Violations ............................................................. 30
Mistake 10: Not Consulting With Credible Authorities on Implementing HIPAA .......................................................... 33
HIPAA Program Highlights ........................................................................ 36
Introduction

Do you realize the average HIPAA Violation is over $50,000 and can include up to a year in prison? Violations are becoming more prevalent and the chance of a random audit is increasing monthly as we approach the new health care laws passed under the current administration.

Today is a perfect time to get your facility compliant and stay ahead of the ever changing laws regarding HIPAA and HITECH Act. Our goal is to keep you informed with monthly law changes, form updates and new violations.

We know there will be drastic changes to HIPAA/HITECH in the next 12 months so we have prepared this quick read on the 10 Most Common HIPAA Mistakes. This may help avoid costly violations but it does not cover everything needed for compliance. We assure you it doesn't cover all of the potential issues a facility might encounter but it's a good start in preparing an office against the most common issues.
**Special Offer**

“Are you prepared to spend hundreds of hours filtering through all the changing HIPAA/HITECH Omnibus rules about to come into effect? Do you have all the needed forms? Is your office out of Compliance? Do you know if it is or not? We have the solution.”

[www.hipaacompliance.org](http://www.hipaacompliance.org)

We have turned HIPAA LAW into a cloud based OFFICE PROCEDURE. Within 30 days, your facility will be a 100% compliant and stay compliant with the help of our trademarked "Compliance Meter".

---

Due to drastically changing health care laws and Omnibus laws coming in September we have designed an incredible membership offer. Get our entire HIPAA Office System and all the cost and time saving features for as low as $497.00 and $47.00 per month. Please check our plans to find the one that's right for your facility.

**Special Offer:** Enter "HIPAA13" in the coupon code box at checkout and receive an additional 5% off the initiation price.
Mistake 1: Not knowing what being a "covered entity" means

HIPAA applies to all businesses or organizations classed as a covered entity. Many businesses assume that they are not covered entities because they have no direct contact with medical records - that could be a fatal mistake to make. Jumping to conclusions such as that can lead you into trouble with HIPAA conformance, and cost you a great deal of money.

The definition of a covered entity is provided below. There are some very obvious covered entities, such as hospitals, medical practices, and dental practices and some not so obvious, such as schools and other establishments holding any form of medical information on an individual. Others include employers that have been provided with medical information, but only if they disseminate that information electronically.

There are some that would not believe themselves not to be covered entities, but actually are.
You are a covered entity if you collect, store or disseminate information that is connected with the health of individuals, whether that is one individual or several. You are also covered if you offer support or services to those that provide such services.

Examples include paramedics, pharmacies, dental practices, health insurers, health care clearing houses, social workers, blood, sperm or organ donor banks and anyone businesses that directly bill third parties for medical costs. Even providers of the software used to store medical information are covered entities, as may be providers of prosthetics.

Let's have a closer look at those who may feel they are not covered. 'You' in these instances refers to you personally, your business or an agency.

Health Care Providers

If you provide payment, bill or receive payment for health care as part of your regular business, then you may be a covered entity. If you also transmit or send any transaction relating to health care electronically, then you are a covered entity.

Health care providers are advised to assume that they are covered unless they take professional advice on the question. If you do not email or otherwise electronically send such files to another party, then you are not a covered entity.

Health Care Clearing Houses

If you or your business or agency facilitates the processing of health information between standard and non-standard formats or content, AND if you do so for another legal entity, then you are a covered entity and must comply with HIPAA.

Health Insurance Plans
a) Individual and Group Private Health Plans

To be a covered entity, a private health plan must provide or pay for the cost of health care. Situations where a plan is NOT a covered entity are:

- It does not pay for the cost of health care,
- It does so but is self-administered, AND has fewer than 50 members,
- It is a long-term care plan providing only fixed indemnity policies for nursing homes
- It is a long-term care plan providing only excepted benefits

Situations where an individual or group private health plan IS a covered entity are:

- It is a group health plan, either not self-administered or with more than 50 members,
- Is a health insurance issuer,
- Is an issuer of a Medicare supplemental policy,
- Is an HMO (Health Maintenance Organization plan),
- Is a multi-employer welfare care benefit plan

b) Government Funded Health Programs

The same basic considerations apply with government funded programs.

You are NOT a covered entity if your plan is not a listed government health plan, and:

- Does not directly pay the cost of medical care,
- The principal purpose is not the direct provision of health care
- The principal purpose of the plan is to provide grants to fund the provision of health care,
- The principal purpose is not to directly provide or pay the cost of health care (e.g. a scholarship or prison system).
- The program provides ONLY excepted benefits

You ARE a covered entity if:

- The plan is a listed government health plan,
- The plan is a high-risk pool,
- The plan is an HMO,
- The plan provides or pays for the cost of medical care, and does not meet any of the excepting qualifications above.

Other than the above qualifications, any business or organization that electronically stores and transfers health information, internally or externally, is subject to the HIPAA regulations. If you are unsure whether you are a covered entity or not, go through the above lists and determine whether or not you are covered.
The vast majority of businesses and organizations that handle health information will be subject to HIPAA. A health care transaction is defined by HIPAA as practically any information transaction relating to the health of an individual, including inquiries between health care providers and health plans or between health plans, for information relating to the eligibility of an individual to receive health care under the terms of the plan, information on benefits of the benefit plan or a response to a request for information on any aspect of the health or health records held by any firm or organization.

Also included is transmission of data relating to the status of any health claim or payment, and the transmission of the undernoted from a health plan to a health care provider's financial institution or the health care provider:

- Payments
- Information on fund transfers
- Information on payment processing
- Explanation of benefits
- Remittance advice

In fact, any information that relates to the health of an individual, including information revealed on a health insurance form, is regarded as covered information, and any transfer of that information by electronic means is regulated by HIPAA.

If you are uncertain as to your status regarding HIPAA registration and conformance as a covered entity, then you should seek specialist help because the consequences of non-conformance can be severe.
Mistake 2: Failing to Comply With the Security Rule

Several years ago, in 2005 to be precise, regulations regarding security measures for health records distributed and stored electronically came into force. A large number of organizations have yet to put the measures into place that will enable them to comply with these regulations.

They have no compliance to security rule procedures and their security rule procedures and policies do not yet enable them to comply with the terms of HIPAA. Not only that, but in order to comply with the security rule, document updates have still to be made, and changes made to business associate agreements. It is important that these oversights, or the lateness in maintaining such updates, are attended to because Medicare and Medicaid Services have announced their intention to audit firms and health organizations to ensure that they are complying with the Security Rule.

By making sure that this is being done, and that any HIPAA compliance procedures already in place have been updated to include the new Security Rule, you should be safe should you face such an audit. Any program that has not been updated since 2005 is unlikely to be compliant with the stringent terms of this part of HIPAA regulations.

In fact, the security rules relating to electronically stored health information have been in effect since 2005, and if you do not yet have policies and procedures in place regarding the security of such records then you are not in conformance with HIPAA. Even if you put such processes and procedures in place, all security plan/policy documents and agreements with business associates must also be updated as appropriate.

A failure to comply could be costly to you, given that the Center for Medicare and Medicaid services has started carrying out audits to ensure such compliance. Although business associate agreements instituted since 2005 will likely conform to HIPAA, those arranged prior to 2005 may not have been appropriately amended.

What is the HIPAA Security Rule?

The HIPAA Security Rule relates to electronic Protected Health Information (PHI), and although this encompasses only a small part of the terms of the HIPAA Privacy Rule, it is highly technical, and easily misunderstood. Fundamentally, the Security Rule relates to three specific forms of security:

1. Administrative Safeguards

Administrative safeguards refer to office procedures, training of staff and any other administrative factors involved in the detection, prevention and correction of security violations relating to electronically stored health records. You must appoint a security officer who is responsible conceiving and implementing the security procedures for your business or organization. The security officer should also be responsible for preventing and detecting security violations, and for correcting any violations of the HIPAA Security Rule.
For example, you must ensure that employees have access only to the electronically processed health information (ePHI) relevant to their work, and that effective employment screening is applied prior to employing such individuals. All of this should be recorded, and relevant procedures audited. HIPAA auditors will also expect you to have provided sufficient training to employees so they understand how the Security Rule affects them collectively and personally. Failure to provide such training is a failure to comply with the HIPAA Security Rule.

2. Physical Safeguards

Physical safeguards refer to the procedures that control physical access to records or ePHI. Even access to geographical areas where such records are stored, such as access to the room by means of a door lock or any other recognitions system such as fingerprint or retinal scan. Examples include recording when keys are issued, to whom and when they are returned.

There may be restrictions placed on the computers or workstations able to access such information, and passwords should be secured by maintaining records of individuals with passwords enabling them to access relevant health records. Such health information need not be complex or overly revealing, but as simple as a change of appointment: this information should be subject to the same security rules as any other medical information. There are many more examples, and the best way you can likely conform to the stringent requirements of the HIPAA Security Rule is to hire a third party to do it for you or utilize software specifically designed to enable you or your business to conform.

If you are interested in more information on how to avoid the strict penalties of non-compliance with the Security Rule, or any other HIPAA regulation, then you can get more details here:

HIPAA Security Rule Conformance

3. Technical Safeguards

The technical safeguard required of the HIPAA Security Rule involves password security and encryption. This not only refers to the security of passwords, and how they are kept safe and frequently changed, but also how all sensitive information relating to patients' personal information is made secure and removed from any storage devices when these storage devices are transferred between computers or users (hard disks, USB memory devices and SD memory cards are three examples).

The Security Rule mentions eight implementation specifications, and unless you are aware of each of these, and how they affect your business or organization, then you may have problems with an audit. Data retrieval is one, and how data is retrieved from faulty storage devices, or devices damaged during power outages or thunderstorms.

These administrative, physical and technical aspects of the security of an individual's electronically processed health information are the major aspects of the Security Rule to which you must conform. Additional to these, HIPAA also focuses on two more aspects of health records security:

Organizational Security
This relates to business contracts, agreements with associates and so on. You must make sure that your business associate is not in breach of the security of an individual's electronically stored personal health information. You must also be able to demonstrate that this is the case, and that you have taken the necessary steps to establish this. If a business association is in breach of HIPAA, then so are you! In such a case, the HIPAA Security Rule requires you to either terminate any arrangement, whether contracted or not, or report the situation to the HHS.

**Policies, Procedures and Documentation**

Fundamentally, you must record all security policies, the procedures devised to implement them, and to document any revisions to processes and procedures. You must also record any detected non-compliance together with remedial actions taken to ensure compliance. For example, if a complaint is made by an individual regarding the privacy of their health records, the complaint and any actions taken must be documented.

Not just that, but HIPAA covered entities must also have written procedures in place that are able to deal with such complaints. A lack of this type of documentation infers non-compliance to the HIPAA Security Rule and you will be subject to prosecution and penalty.

Another obligation in this respect, particularly in connection with health plans, is that organizations must inform plan members of their Security Policy at least every three years, and inform interested parties where to obtain it. This can be done by providing a physical copy by post, providing an internet link in a newsletter or even simply reminding the plan participant that the policy exists.

You should take professional advice for all of these aspects of the HIPAA Security Rule because the penalties for non-compliance can involve a fine of $1 million, imprisonment for responsible individuals and termination of contract with professionals such as doctors and consultants. You can find such advice on our website at:
Mistake 3: Not Taking the Time to Train and Retrain Employees

It is absolutely critical that you invest the time and energy needed to properly train your employees in the requirements of HIPAA. Sure, in the early days of HIPAA, employers trained their employees, but that was it. Very little, if any, refresher courses were provided to cover amendments to the Act, and in many cases new hires did not receive the degree of training originally offered to existing employees.

HIPAA requires that new employees with access to electronically stored health records receive the HIPAA training relevant to their position in the organization. Not only that, but retraining is required in cases where regulations are amended or additions made to the original privacy policy. Training is not only needed to familiarize employees with the general terms of the regulations, but individual training is essential for those with specific responsibilities in respect of the security of electronic health records.

Examples of HIPAA Training Needs

a) General Awareness
Irrespective of their function in a business or organization classed as a 'covered entity', all employees should be made aware of HIPAA and what it is intended to achieve: the privacy and security of people's health information as stored or communicated electronically. This general education should be provided to every person you employ, whether or not you have identified employees as having a direct influence on such security. It is difficult to determine employees to whom such training is irrelevant, since secretaries, receptionists and even cleaners may find themselves able to gain access to protected information.

b) Individual Specific Training
Individuals should be provided with training relevant to their specific function, both within the organization and with respect to their function in that organization's HIPAA policy. For example, employees nominated as auditors, whose function is to carry out internal audits of the organization's compliance to HIPAA, must be thoroughly trained, not only in the terms of the regulations themselves, but also in the skills of auditing.

c) IT Personnel Training
IT personnel should be trained in how to maintain security of electronic records, not only in terms of their storage, but also of their dissemination and communication. Telephone systems, both landline, cell and VoIP can be hacked and who in your organization is trained to prevent it? Answering services may archive messages and conversations that are encompassed by HIPAA, and employees of these services should undergo suitable training in HIPAA privacy rules. If you are a covered entity, you may perhaps feel bound to request this form of conformance on behalf of answering services that deal with your electronic communications.

d) Security Maintenance Training
Maintenance staff must receive regular training, particularly those responsible for maintenance within the realms of IT equipment and physical security equipment.
such as locks and intruder alarm systems. Hard disks, floppies, USB storage devices, SD cards or any other electronic storage media used to store private health information must be stored in secured areas. Every employee with access to these areas must receive HIPAA training which refreshed on a regular basis as necessary.

These are just a few examples of how training should be split between the general and the specific. Everybody should be HIPAA aware, and those with specific functions should receive training targeted to how the Act impacts on their function within the organization. Records of all training should be maintained, and included in the regular HIPAA auditing procedure.

**HIPAA Training in Practice**

Fundamentally, general training and education will focus on the need for privacy relating to electronically stored health information, the extent of such privacy and in the privacy policy of their own establishment. It should then proceed to explain the various types of record held by the business, the types of security used to prevent misuse of patient data, and the consequences of breaches of HIPAA: both corporate and personal.

To put it in simple terms, HIPAA training should inform employees what the Health Insurance Portability and Accountability Act of 1996 is and is intended to achieve, what their company or organization is doing to achieve that, and what their part is in all of this.

Every employee within any organization that is classed as a covered entity should be made fully aware of their responsibilities with respect to HIPAA, how they are expected to play their part, and of the consequences of failing to meet these responsibilities. They should then be fully trained so that they are capable and qualified to play that part effectively and efficiently.

**How to Carry out Training**

How should HIPAA training be carried out? It can be provided either through a traditional classroom setting, offsite or on the company or health service premises, or electronically through a dedicated online service or by means of computerized training schedules that employees can take when convenient.

There is no formal method laid down by which training should be provided, and each covered entity can decide itself how to go about it. It is the end result that is important, not how it is attained. Some establishments train their employees using in-house instructors, others carry it out in-house using contracted trainers and yet others send their employees to off-site training courses. Which you use will likely depend upon how familiar individual employees must be with HIPAA; thus a HIPAA auditor or manager will require more intensive training than a dental technician.

**Training Software**

It is often more convenient to use training software, that each employee can use when convenient and at a rate to suit them personally. If your business or organization is a covered entity and must be HIPAA compliant, and your employees
require specific targeted training in specific aspects of the Act, Click Here for further information on the training we can provide.

By putting your employees through a HIPAA Compliance Course, you will be able to obtain HIPAA certification which is essential for any business, company or organization that holds electronic health records. You are also advised to appoint a HIPAA liaison officer, to whom employees can turn if they have any questions regarding their part in the security of health records.

A written manual, detailing the processes and procedures involved in your HIPAA Policy will also help to persuade authorities that you have done all you can do to ensure that your employees are all trained with regard to their part in your policy.

More information on this can be found on our site HIPAA Compliance
Mistake 4: Ignoring State Privacy Laws

Although HIPAA is a federal law, and will therefore preempt state laws, there are a few exceptions that you must be aware of. These exceptions are generally more restrictive than the terms of HIPAA itself, because the law in this situation is that if a state law is stricter than a federal law, the state law prevails.

For example, if a state law is in place to prevent fraud with respect to health records, or if it assists in the delivery of health care, then that law can supersede HIPAA if the terms of the latter are not as encompassing or as restrictive as the state legislation. It is crucial that if you are a covered entity then you must make yourself aware of the state law appertaining to privacy protection of medical records.

If the laws of your specific state can in any way hold sway over the federal law, then it is your responsibility to know that: ignorance of the law is no more an excuse in respect of health privacy and security laws than it is of any other situation where federal legislation is more lenient or less restrictive than that of your state.

When State Law Preempts HIPAA

Many have difficulty in understanding the difference between the two, and when federal law preempts state law and vice versa. Here is some clarification on that matter, although it is easy to understand how it can be confusing, particularly in regard to the Privacy Rule.

1. If state law contradicts HIPAA, then the latter applies, not state law. The state cannot pass laws contradictory or contrary to federal law.

2. If state law is more stringent or rigid than HIPAA, then state law will apply. It is thus possible for HIPAA to be applied differently between states, although the initial tenets of the Act will be the minimum that can be applied. So, state law can be more exacting, but not more lenient, than the original Act.

Where you find state law and HIPAA to be contrary to each other, you can generally assume that state law is the more stringent and will apply. You should therefore make sure that your HIPAA compliance is to both the federal Act and to state law. If there is a dispute or doubt on a certain aspect of HIPAA as to which is the more stringent, then you will not be able to resolve that yourself. That will likely be a matter for the courts.

Conform to Both for Safety

While it will be possible to take professional advice on the matter, defending your case would likely be extremely expensive. Ignoring state privacy laws could cost you a lot of money, even if you were ultimately proved correct in law. It is therefore wise to ensure that you conform to both: one will be more stringent than the other, so by conforming to what you perceive as being the more exacting of the two laws you will, by definition, meet your legal obligations.
Such legal disputes are frequently arguments over semantics, and irrespectively of how they are settled, you will ultimately have to conform to the terms of the more rigid and exacting of the two regulations - whether that is HIPAA or your local state regulation. The important thing is to be aware of your state's version of a specific HIPAA regulation.

**What Are the Differences - What to Look Out For?**

What should you be looking for when trying to establish the difference between federal and state law regarding health record security? The main differences are generally not in the meat of the law, but with reference to public health, and reporting requirements. For example, laws that relate to infectious or communicable diseases, local records of births and deaths child abuse and so on - factors that have a predominantly local bias. These factors are often state-related, particularly with respect to how such information is shared, communicated and recorded. In fact, the HIPAA Privacy Rule offers guidance on the application of state law.

**Electronic Health Record Security Rule: The State Vs HIPAA**

Most confusion is liable to occur with the HIPAA Security Rule. This relates to the security of electronically stored health records, where HIPAA and state laws may well be in conflict. Many states have their own laws relating to electronic storage of records, and here again it would take a lawyer to figure out which preempts the other.

Your advice here is to learn as much as you can about your state law, but also be aware of exactly what HIPAA asks of you. Then apply the more stringent of the rules as you interpret them and document everything you do. Document your Security Rule policy, the safeguards and security you have put in place, and also the training procedures and everything else you have done to meet the terms of the Security Rule.

It is likely that, if you can demonstrate that you have tried your best to meet the regulations in good faith, then irrespective of whether that meets the needs of state law or not, it might be deemed that you have meet the requirements of any laws that apply. If you documented your processes and procedures, and can show that you have followed these faithfully (by records, audits, training, etc), although this will not absolve you from your legal liability relating to state law, you may mitigate that liability.

If you do all that you can to safeguard the security of electronically stored health records, and can prove that you have done so by means of records as outlined above, then you should generally be OK. However, states often jealously guard their own laws against federal equivalents, and it may be worthwhile asking your state for advice on training your employees.
Mistake 5: Forgetting to update the notice of privacy practices and/or send the three year reminder

A requirement of HIPAA is that covered entities must inform patients or participants of health insurance plans about how their medical information is used and of their rights regarding it. For example, patients or members of health plans have the right to inspect and copy health information held about them, and also to request amendments if they feel that such information is false or contains errors. There are many more rights listed under the regulations.

You must remind people of these rights every three years, and provide details of how they may obtain a copy of them. You must also inform patients or plan participants within 60 days of any changes you make to your privacy practices, or changes to the plan. For employers, this means that notification of updates will be necessary if any changes are made to health plan insurance cover or to the terms of a wellness program after the initial privacy policy was provided. This also applies to any relevant change to state privacy law.

Never make assumptions in relation to notification of privacy practices. When making attempts to comply with the regulations regarding notification of privacy practices, covered entities will include the privacy notice or details about it along with the open enrollment materials provided. They may assume that this is sufficient to comply, but it might not be - in fact, in most cases it will not be sufficient just to do this.

Where privacy is concerned, HIPAA rules are particularly stringent, and general significantly more so than for other forms of notification. It is very important that you pay particular attention to the HIPAA compliance rules when it comes to privacy notifications.

It is easy for an employer or covered entity to forget to send out notices informing the relevant people about changes they have made to privacy practices. Such forgetfulness is a violation of the terms of HIPAA. So too is an omission to send out the three-yearly reminder. Even when they send out the reminder, some businesses and practices forget to include a notice on how to receive a copy of the privacy practices.

The HIPAA Privacy Rules generally allow private health information to be used and disclosed to third parties without the expressed prior permission of the subject for the purposes of health care treatment, insurance payments and various health care operations. For example, health information could be provided to the subject’s medical insurance company to ensure that payment will be made for their treatment. The practice or organization holding these health records are obliged to remind subjects of this fact every three years.
It is not unknown for a practice to forget to do this, and if they do then they are in breach of HIPAA. Some covered entities may include the privacy notice as part of the enrollment procedure, or in the description of the plan. However, the HIPAA requirements for privacy notice requirements are generally more stringent than for other types of plan notice, and what is usually acceptable with these will likely not be sufficient for HIPAA.

A typical privacy notice with state something along the lines of:

"Under certain circumstances we are legally permitted to use or disclose your protected health information without requiring your permission."

You can then go on to offer examples of ways in which you may do this, stating clearly that these are examples and not definitive, and that the examples are provided only for the purpose of illustration. Some examples provided could be:

"For Treatment: We may use or disclose your protected health information for the purposes of treating a health condition, and enabling, managing or delivering health care. For example, we may disclose medical information to physicians treating you, or nurses or technicians as appropriate."

"For Payment: We may use or disclose your protected health information to ensure receipt of payment for services we may have provided to you, or about to provide to you. For example, we may contact your health insurer, provider of an occupational health plan or any other body responsible for making payment on your behalf for medical services provided to you by us."

You should also provide information on the subject's own rights, such as their right to inspect, copy or amend certain health protected information that may be used to determine your health care benefits. You should also inform them the steps they must take to do so. You should also inform them that they can request that you contact them regarding confidential medical information only in a specific manner: such as only at home or only by email. Another importance piece of information to be included is how they complain if they believe that their rights to privacy have been violated.

And so on - this is not a sample notice that can be composed without thorough knowledge of the circumstances in which you may have to divulge a subject's protected health information. Most covered entities are advised to have such privacy notices compiled by a third party experienced in this type of work.

You can contact us regarding this at HIPAA Compliance Tools
HIPAA Privacy Rules require that you compile a plan for amending your privacy notice when any significant revision is made. That is, any material revision that changes or adds to any of the provisions or statements provided. An example would be any changes made to the provisions of health plan policy, or anything that will affect the service or benefits you receive. As previously noted, such updates must be provided to participants within 60 days.

It is important that if you are a covered entity, you fully understand the terms of the HIPAA Privacy Notice and that you have a procedure to ensure that they are provided to patients or insurance plan members according to the requirement. The most common reason for non-compliance is forgetting to send the three year reminder or omitting to update the note of changes made to privacy practices.

Such omissions can be very expensive, and you should avoid the possibility of that happening to you.
Mistake 6: Lacking a Written Procedure for Investigating and Resolving Privacy Complaints

Patients and participants in health plans are going to complain about the privacy of their protected health information. When they do, HIPAA demands that you have a procedure in place for investigating and resolving such complaints. It may not specifically state that this should be a written procedure, but that is how it will likely be interpreted.

Complaints can come in a variety of forms, such as a formal notice to the administering body, a letter to your Human Resources department or even a comment made to a member of your staff. It doesn't matter how the complaint is made - formal steps should be in place for its investigation, even if it is an off the cuff remark.

Covered entities may be unsure of the proper steps to take in the event of a complaint, and a written procedure for handling them enables all staff members involved to follow the same processes. A written procedure is the best way to ensure standardization and avoid a fine in the case of inadequately investigating a complaint. Without one, your case will likely not be considered favorably.

An employer should investigate any complaint where there is reason to believe that a violation of any of the terms of the HIPAA Privacy Rule had taken place. A written procedure should cover the following steps in the investigation:

- The allegation which is the substance of the complaint
- The steps taken to investigate the complaint
- The facts revealed by the investigation
- Details of the specific section(s) of HIPAA the facts show have been breached
- Remedial action taken
- Any preventive action taken to ensure that the same cannot happen again

While it is important that the facts of a complaint are established, and any problem or breach of HIPAA has been resolved, it is equally important that steps are taken to prevent any future exposure to a similar complaint.

Privacy Rule violations can be very costly as exemplified by a case in February, 2011, when the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) announced a civil monetary penalty of over $4 million imposed on one private company for failing to produce medical records in a timely fashion on request to a number of individuals, and for failing to cooperate in investigating the ensuing complaints.

This case opened up a few eyes to the way the legal profession interprets HIPAA, and for the need for written procedures in all aspects of the Act: including dealing with complaints!

If you are lucky, the complainant will refer to you first, although they may just go straight to the OCR (this may be more likely now as a consequence of the above
ruling). It will likely count in your favor if the OCR investigates and you have had no complaint directly from the complainant, and also if you can demonstrate that you have a written complaints procedure in place. This is another argument for having such a procedure written down as part of your general HIPAA policy.

Some organizations will have a written HIPAA management system broken down into each aspect of HIPAA, and conforming to the HIPAA Privacy and Security Rules will be one of these. Your complaints procedure should be part of this. If a complaint is made, then the OCR will want to see that you have such a procedure in place and that you may have been able to resolve the problem yourself had the complainant contacted you first.

HIPAA allows anyone to lodge a complaint regarding breaches of the Privacy or Security Rule, although such complaints must be lodged within 180 days of the circumstances of the complaint taking place unless 'good cause' can be provided for this not being done. You are not permitted in any way to retaliate for such a complaint or you will face further action against you.

It is therefore to your advantage, not only to have a written complaints procedure, but also to be aware of the major reasons for such complaints so you can address these before they become an issue. The main reasons for people complaining are:

a) Disclosure of identifiable health information for reasons outside those permitted by HIPAA.

b) A lack of adequate protection for a subject's identifiable health information.

c) Refusing or failing to provide individuals with a copy of their health information records, or to offer them access to it.

d) Disclosing more information than is minimally required to meet the reason for the information initially being requested.

e) A failure to receive the subjects authorization for a disclosure that requires it.

'Identifiable health information' is that which can identify the subject with the information released.

If you focus on making sure that have taken all steps possible to prevent any of the above five reasons for complaint, then you will have gone a long way to ensuring that your business, organization or practice is subject to as few complaints as possible. By documenting these steps, it will stand you in good stead should a complaint be made to the OCR.

Although sanctions may be applied for a failure to meet the terms of the HIPAA Privacy and Security Rules, these will likely be minimal - if applied at all - if you can demonstrate that you have written processes and procedures designed to prevent or minimize these, and that you have already taken remedial action to prevent a recurrence. Maximum sanctions are applied to those that fail to cooperate with the OCR in their investigations, and fail to take steps designed to improve their protected health record security.

If you need advice on your procedure, contact us HERE

An effective complaints procedure will include:

Copyright © 2010-2013 HIPAA Compliance Tools. All Rights Reserved.
1. Information to subjects on how to make complaints: personally, by telephone, by writing or by email. Offer phone numbers and personal and email addresses to which complaints can be made in your original HIPAA Privacy Notice to them.

2. Complaints should be made to a specific individual, identified by position in your complaints procedure. That person's identity can be named on your website or in the Privacy Notice provided to patients and plan members.

3. The complaint procedure should identify the information required from the complainant. Generally, that should include a detailed reason for the complaint, the date that the incident occurred if relevant, names of individuals involved if known and an address where further communication to the complainant should be made and how it should be made (written, email, at work, at home, etc.).

4. The next part of your written procedure should define what happens next: how you go about investigating the complaint and deciding on its merits. That should include a notice to the complainant letting them know what happens next and a likely time-frame for a response.

Many official complaints to the HHS are made because this information is not provided: complainants send in the complaint and receive no further communication. You may be investigating, but you should tell them you are, and also let them know how long it may take you and when they can expect to hear from you next. Fail to do that, and the next call you get may be from the OCR.

If you do not yet have a written procedure to handle complaints on the HIPAA Privacy and Security Rule, then set one up now. If you need help with this, contact us HERE.

We have experience in formulating complaints procedures for health authorities and businesses of many different kinds.
Mistake 7: Not Understanding HITECH

The HITECH Act (Information Technology for Economic and Clinical Health Act) provides teeth to the civil and criminal enforcement of HIPAA. This Act was introduced to deal with the problems associated with the expansion of electronic storage and interchange of protected health information (PHI) in recent times.

When HIPAA was conceived and initially passed in Congress in 1996, computerization of records and the use of electronic means of communication were significantly less than now. In the modern era, when electronics is the preferred means of communication by most and the only means by many, the electronic storage of medical records is now universal. HITECH is intended to widen the scope of the Privacy Rule and Security Rule of HIPAA to account for this, and in doing so it increases the potential for legal liability for non-compliance.

If you are unaware of HITECH, or do not understand it, then you can almost certainly anticipate problems with HIPAA farther down the line. HITECH introduces new provisions such as:

- Where health records are stored electronically, individuals have a right to obtain their protected health information on request in an electronic format.
- Some HIPAA provisions now apply to business associates.
- There are additional requirements relating to such as marketing communications and accounting that significantly modify HIPAA.

The provisions of HITECH are patently intended to enhance the enforcement of HIPAA and catch those that until its introduction were failing to apply the Privacy and Security Rules effectively.

It almost certain that any HIPAA compliance and policy procedures you have put in place prior to the introduction of HITECH in 2009 will have to be updated. Any systems or programs you implement with regard to HIPAA, or any forms designed relating to these, must be updated and modified to include the provisions of HITECH or they will not conform to HIPAA.

Make Best Use of HITECH: CHECK HERE NOW

Key Provisions of HITECH Relating to HIPAA:

Willful Neglect Sought Out and Punished
Mandatory penalties will be imposed for "willful neglect" of HIPAA. Those who have not tried very hard to comply with HIPAA will be at significant risk of detection and punishment. Prior to HITECH, HIPAA non-compliances were not rigorously hunted down and prosecuted, but now they are more likely to be. Penalties can extend to $250,000 for a single offence to over $1 million for repeat/uncorrected offences.

Business Associates Included
In some cases, the civil and criminal penalties applied under HIPAA will now apply to business associates. Although HITECH contains no provision enabling individuals to
bring a cause of action against providers, state attorney generals may do so on behalf of their states’ residents.

**Regular HHS Audits**

HHS must now carry out regular audits of covered entities and their business associates to ensure compliance with HIPAA.

**ePHI Access**

Where a provider of a health service maintains patient or member records in electronic formats, the subject has the right to request a copy of his or her protected health information records in electronic form - that is referred to as ePHI. The individual can also request that ePHI is provided to a third party. The fee applied for this can charge only the labor cost involved.

**What HITECH Means to You**

What HITECH means to you is that first of all you must be aware of it, particularly if you are a business associate of a covered entity that has to date been relatively unaffected by HIPAA. Here are some specific that you should be aware of:

**Breach Notifications:**

Patients must be notified of any unsecured breach of the Privacy or Security Rules. If this breach affects 500 or more patients then the HHS must also be informed. This will also mean that that the entity causing the breach will have their name posted on the website of the HHS. In certain situations, local media may also have to be notified. The above is the case whether the breach occurs due to internal or external factors.

**The Need for Electronic Transmission of ePHI:**

Covered entities will be required to be able to readily transmit PHI records electronically on request. Providers who store records electronically may not necessarily have the facility to achieve this, although it must be understood that in the current era of immediate electronic communications such requests will become the norm rather than the exception. You should therefore make sure that your organization or business is able to conform and provide ePHI immediately upon request. Request for paper copies will gradually reduce in favor of ePHI.

**Business Associates:**

Business associates can no longer dodge complying with HIPAA. Under HITECH all business associates must comply. For example, the majority of software vendors will now clearly be classed as business associates. In the past, HIPAA privacy and security requirements applied to business associates only through their contracts, and many of these contracts did not specifically do this. This no longer applies, and HIPAA might now apply to most business associates irrespective of the terms of their contracts. Business associates must also report security breaches and there are several other aspects of HIPAA that will apply under certain conditions.

**The Bottom Line**

The bottom line is that the responsibility for HIPAA will be shared between providers and business associates, and that the concept of the 'business associate' will finally become a real one for many small providers. There are many more aspects of
HITECH that apply to providers of health services and insurance plans, and that will involve modification of the HIPAA policies of these providers.

Additionally, the factors discussed above refer only to a small part of the extent of influence of HITECH as it applies to HIPAA and are not comprehensive by any means. The major reason for this information is to express that HIPAA is now being implemented and enforced more comprehensively than it has been, and that medical and health service and insurance providers and their business partners have significantly more to be aware of in this respect.

HITECH offers incentive funding using taxpayers' money to offer incentives for providers to adopt an EHR system. More transparency and accountability is an inevitable consequence of this. Any provider wishing to benefit from these incentives, or even just wants to avoid the penalties for non-conformance, will have no choice but to become more educated in the provisions of the HIPAA Privacy and Security Rules and the new provisions of HITECH.

More details on how You can Conform to HITECH and HIPAA are available here: Click
Mistake 8: Being Uninsured for HIPAA Investigations Against Business

Being uninsured for HIPAA investigations can cost your business a great deal of money. In 2009, a civil monetary penalty of over $4 million was imposed on a business by the HHS for a breach of the HIPAA Privacy Rule: could your business or organization pay such a penalty without folding, or at least without seriously disturbing your shareholders?

Not only that, but the introduction of HITECH in the same year (2009) has given larger teeth to HIPAA, and it is more likely that health services, businesses and organizations that hold protected health information in electronic form will be more frequently audited and non-conformances hunted out and prosecuted.

The fact that HITECH has brought businesses associates of covered entities more securely within the HIPAA fold has also resulted in a greater potential for prosecutions under the HIPAA Privacy and Security Rules. So are you sure that you are insured for HIPAA violations? Many professional liability insurance policies and business own insurances do not carry HIPAA coverage unless you have specifically requested it.

You must make sure that you full understand what range of insurance cover you have, because it could cost your business or your job if you are not covered for HIPAA non-conformance or for complaints made against you by patients or members directly to the OCR - the Office of Civil Rights of the Department of Health and Human Services.

If the HHS opens an investigation against your business, practice or facility, then the cost of hiring the attorneys is going to reach several thousand dollars simply to respond to the HHS in legal terms. Then if there is any financial penalty imposed upon you, it would be nice to know you are also insured for that. HITECH has given a warning to all health service providers and insurers that any non-conformance of HIPAA will be sought out and prosecuted - and the example cited in the first paragraph shows that they are after the blood of those that ignore the terms of the HIPAA Privacy Rule or Security Rule.

If you are a covered entity you should make sure that you have an insurance policy to cover at least investigations and responses to claims and complaints under HIPAA by your patients or members. The premiums to cover you for this are generally small, and you will be glad of the cover should the need ever arise.

More expensive is coverage for financial penalties. Prior to HITECH, the maximum penalty that the HHS could impose for a breach of HIPAA was $100 for each violation or $25,000 for all identical violations. HITECH increased this to up to $50,000 for a single violation and maximum of $1.5 per year. HITECH also enables penalties to be assessed even when the covered entity was unaware it was in violation of HIPAA, unless the violation is corrected within 30 days of it being discovered. This was not possible prior to HITECH because the covered entity could bar the imposition of financial penalties for contraventions of which they were unaware.
It is now not only more likely that you will be found out if you are failing to conform to the requirements of HIPAA, but also more likely that any excuses you have for that non-conformance will be ignored in determining your civil or criminal liability in the event of any serious leakage or exposure of protected health information.

It is also more likely that the penalty will be high and punitive, in order to make sure that:

a) you are punished for the breach,

b) that you have no further breaches and

c) the health service and insurance industries at large understand that they must conform to HIPAA or suffer the consequences.

If you are uninsured for an HHS investigation, you will be less liable to be able fight it and offer competent legal arguments against any negative findings. If you are positive that you are in conformance with HIPAA in all respects, you would be able to respond to such an investigation if you could afford professional legal representation. You should therefore check with your current insurer whether or not you have the appropriate insurance cover. If not, then check up on the costs of adding that to your existing policy.

Simple reading your policy 'small print' might not be sufficient for you, because semantics can be critical in the legal business. For example, you may be covered for the consequences of 'a wrongful act' - but what does that mean? Does it cover breaches of fiduciary duty under HIPAA and HITECH? If it does so, what are the limits of financial responsibility? Are you covered for both legal costs and the cost of any penalties or fines imposed?

You can find your business under investigation at any time if a patient feels that their health information has been released. A dental receptionist can make a misunderstood comment, and rather than complaining initially to the dental surgery, the complaint goes straight to the OCR. They are then obliged to carry out an investigation. If this is not the first complaint regarding your business, then you will likely require some legal representation, not just to defend the case, but to establish whether or not the investigation is properly justified.

That’s just an example, and there are many others. However, one fact that cannot be disputed is that since HITECH in 2009, any suggestion of a violation of the HIPAA Privacy Rule or Security Rule will be vigorously pursued, particularly if made by more than one individual against a specific health service or plan. It pays to make sure that your insurance policy covers the cost of your legal representation, and even more if it covers the cost of any financial penalty imposed.

The same is true if you are a business associate of a covered entity. If you supply software to a hospital that is used to store patients' records, then you are a business associate and subject to HIPAA, and may require personal liability insurance that includes HIPAA violation cover. If you maintain such electronic storage equipment you are also a business associate and that also applies if you supply the locks and other security equipment that help maintain the security of the protected health information.
In fact, if you supply any equipment, materials or services that appertain to the security of protected health information, or in some cases even to businesses that do provide such equipment and services, then you also should make sure that you comply with HIPAA and are insured for any breaches. Ignorance of the regulations is no excuse, as HITECH makes quite clear.
Mistake 9: Oral Privacy Violations

How often have you heard a doctor or nurse discuss another patient's health details in a public location? A common thing to happen in public wards containing more than one bed is for consultants to discuss health details in the vicinity of patients lying in an adjoining bed - this is in contravention of HIPAA.

HIPAA states that covered entities, including doctors, nurses, consultants and health facility managers, must respect a patient's medical privacy by not discussing the patient's condition or treatment orally when the identity of the patient can be known. This occurs every day in hospital wards, dental surgeries and even in some pharmacies when one staff member comments to another on a case or course of treatment when the patient is easily identifiable.

If the patient cannot be identified, then this is not regarded as a breach of the HIPAA Privacy Rule, but in many such cases the patient is lying or standing beside the 'informant' and there is now doubt who is being referred to.

What is Identifiable Information?

HIPAA states that covered entities such as doctors and nurses must respect a patient's medical privacy by not orally disclosing identifiable information when not in a private location. But what is 'identifiable information'? Must it name the patient or subject by name? Is it sufficient just that the identity of the people being discussed can be assumed or deduced from a description of their conditions or even their family circumstances? What defines 'identifiable information'?

This is a difficult situation to interpret beyond doubt, and it’s astounding how many trained medical professionals discuss a patient to another staff member when they are in earshot of a family member, another patient a member of staff not authorized to hear such information.

The rules state that that a patient's medical information should be discussed privately when there is no chance of others hearing the discussion and relating the information at that time or at a later date with the information being discussed. That renders illegal the old ward-style discussions of a patient's case, with the consultant discussing the case with nurses and perhaps trainee doctors in front of the patient with other patients lying on their beds either side.

Before trying to determine how to avoid such violations - and at first glance the only way to do that would appear to be not to discuss the patient's case at all except behind locked doors in a soundproofed room - we should first take a look at what the regulations actually say, because this appears to be a very restrictive rule and open to anybody with a litigious mind to claim compensation for even one loose word spoken in public about their condition.

What HIPAA Says About It
This rule caused so much confusion and so many problems in the early days of HIPAA that HHS amended the Privacy Rules in 2002. Incidental oral disclosures can now be allowed that:

- Cannot reasonably be prevented,
- Is of a limited nature only and,
- Is a by-product of an otherwise permitted use

It does not require that health facilities provide soundproof rooms or that doctors and nurses stop talking about their patients. However, they should provide reasonable security regarding their patient's health information and carry out such discussion in public places where others could overhear what is being said.

HHS has stated that the privacy rule should not prevent healthcare providers from talking about or to their patients, and states that the primary consideration is the health and appropriate treatment for the patient. However, reasonable safeguards should be taken to prevent oral communication from revealing a patient's protected health information to others. Healthcare providers will not be pursued for oral contraventions of the HIPAA Privacy Rule, but ONLY if they have taken all possible steps to avoid such a contravention.

This is very open-ended, and it is difficult to ensure that any verbal communication you have regarding a patient, either with the patient, another professional or even by telephone, cannot be overheard by another. Keep in mind, however, that it is not a contravention of HIPAA unless the patient can be connected with the information overheard. However, this connection can be so easily made that HIPAA regards it as a violation if health information is made public to unauthorized people even without this connection being made obvious.

Unauthorized Conversations

For example, if a doctor’s receptionist is discussing a patient's condition with a member of the public without stating the identity of the patient, this is still in violation of HIPAA because one of the parties is not authorized to receive private health information, irrespective of whether the identity of the patient is revealed. If another overhears the conversation, that is less apparent because the information is not deliberately being imparted to unauthorized ears.

One way to avoid violating this oral aspect of the HIPAA Privacy Rule, therefore, is simply not to discuss private health information with anybody else unless it is essential, and certainly not to do so in a public place, even to authorized personnel. Some health establishments try to overcome this problem by the use of white noise and acoustic wall and ceiling tiles that absorb sound and prevent reflection.

Why is Oral Privacy Part of HIPAA?

HIPAA refers to electronically stored private health information, so what does this have to do with oral communication of health information? Many people believe that by covering oral communications, the HHS has gone beyond the original mandate that was to be restricted to electronically stored and communicated records.
By including oral communications the number of potential violations is staggering, and several non-conformances could occur every single day. However, by making people aware of this form of non-conformance, and making the discussing of private health information with unauthorized personnel or the public a disciplinary matter, it can be largely controlled.

Another problem these days is the use of social media, which is another breeding ground for HIPAA violations. It is exceedingly difficult to control the dissemination of information on social sites such as Twitter and Facebook, but that is another problem!
Mistake 10: Not Consulting With Credible Authorities on Implementing HIPAA

The internet is full of opinion and misleading information, and there many overnight businesses that claim to be experts on HIPAA. It is important that you make sure the source you use is chosen carefully, and that you understand who you are dealing with. You should deal with a reputable firm that understands HIPAA and the importance of properly observing its directives.

HIPAA Statistics

According to an analysis by HIP/SA of OCR’s breach statistics, about 11.5 million patients had their medical records breached in 292 events from June 17, 2011 through July 17, 2011. The leading cause was theft of information followed by unauthorized access or disclosure. Business associates were involved in 58 of these breaches, supporting the regulations in HITECH that increase the responsibilities of business associates in conforming to HIPAA.

Theft of information held on laptops was a major contributing factor in these statistics, indicating the need for better security of laptops containing protected health information. In fact, the question should be asked if PHI should legally be held on portable storage equipment rather than be accessed remotely from it.

Another major factor, second only to laptop theft, was loss of paper records. This also supports the feeling that PHI should be stored on secured and encrypted static storage devices rather than on laptops or in paper format. California, Texas and New York State had most reported breaches, although that should not be surprising given their populations.

These are the statistics, and are why conforming to HIPAA is so important. 11.5 million people is a large number to have had their private health information compromised, whatever the reason, and is one of the reasons why HITECH was passed to support HIPAA and increase the penalties for non-conformance and serious breaches.

Education is Important

However, penalizing people is not always the right way to ensure conformance, because frequently it is due to a lack of education. If people do not understand HIPAA and what it is really trying to achieve, then they cannot be expected to properly implement and maintain it. This is one area where we can help you: we can not only help you to implement HIPAA, and properly maintain your privacy and security systems, but we can also teach you what HIPAA is about, and the important of maintaining private health records.

The above statistics are appalling, and it is extremely important that if you are a covered entity you implement HIPAA as effectively as you can. There is no quick fix to speedy implementation. HIPAA and HITECH together must be implemented properly, one step at a time and you must miss nothing and leave no loophole open.
through which errors can be made and contraventions allowed to occur without them being caught.

**Audits and Reviews**

Your systems should be regularly audited by trained internal auditors, and by holding quarterly HIPAA review meetings for example, you can review internal audits carried out to ensure that your HIPAA procedure is running smoothly. Any non-conformances revealed can be discussed along with the remedial actions taken to resolve the immediate problem and to prevent any recurrence.

HIPAA software can be used to run your HIPAA management system, and such software also ensures that you miss out nothing and that all necessary records and forms are maintained as they should be. Flags will be used to warn you when regular actions are due, such as monthly internal audits and review meetings.

The above statistics indicate the importance of meeting your obligations with respect to HIPAA and we can help you to implement HIPAA so that it meets all the regulations and also of HITECH as it impacts on HIPAA. This is a very important aspect of HIPAA that must be taken very seriously because a breach can be costly - both in human terms to those whose records are at risk and in financial terms should you be prosecuted for a non-conformance or a breach of the Privacy Rule or Security Rule.

**Bad Publicity Can Hurt**

However, it is not just the breach that might be your main problem, but also the publicity that can be given to such non-conformances, particularly where they impact on the individual and his or her private health information. The public tends to be very protective of its health details, and do not take kindly to them being made public or even in knowing that individuals or unknown organizations have acquired them from those trusted to keep them safe.

That could impact severely on the future health of your business or organization, if it became publicly known that you were unable to maintain the security of the private health information entrusted to you. By making the correct decisions with regard to HIPAA implementation and maintenance, you can avoid such problems and be regarded as secure and worth entrusting with such personal information.

**Choosing the Right HIPAA System**

In other words, the fewer HIPAA breaches, the more businesses you can expect. Choosing the right system to run your HIPAA processes and procedures can pay for itself many times over. This is a very important set of regulations that should be given the care and attention necessary to ensure that it is set up right from the beginning. HIPAA is a living process that is continually changing and requires continual maintenance and monitoring.

Along with HITECH, HIPAA is the most important piece of legislation to hit the health and medical services and health insurance industry for the past few decades and should therefore be treated as such. Make sure that you use a credible authority when implementing HIPAA - it is too important to your future to do anything less.
Check out how we can help you to make sure that your HIPAA processes and procedures conform to every regulation, and that you can be sure you have done all you can to avoid non-conformance or breaches of the HIPAA or HITECH regulations.

Contact us here for more information on how we can help you implement and maintain your HIPAA procedure.

HIPAA Compliance Tools
HIPAA Program Highlights

Features Included:

- 54 policies of which 23 are Privacy
- 76 procedures of which 23 are Privacy
- 73 customized forms, with PDF, Word Doc and Excel format
- Personal Helper to assist in all compliance projects and forms
- Simple step-by-step process monitored by helper
- Compliance Meter™ to insure compliance is maintained
- Monthly task lists and documentation

Monthly Membership Benefits:

- Automatic Law Upgrades including form revisions at no extra cost
- Customer Support including access to a Helper to answer questions
- Monthly newsletter reporting new legislation and recent violations
- Continuous updates on Obama Care sent via cloud as they occur
- No renewal fees, simply pay the membership and never lose benefits
- Customer support in the event of a HIPAA or HITECH Audit

Why you need this program:

- Saves research hours trying to keep up with law and form updates
- Saves money purchasing forms and upgrading laws and procedures
- Provides staff with super quick and easy reference materials & forms
- Removes all uncertainty and allows staff and Drs. to spend time on patients
- Protects clients data and provides insurance coverage for violations

100% Money back Guarantee if not totally satisfied

Take me there www.hipaacompliance.org