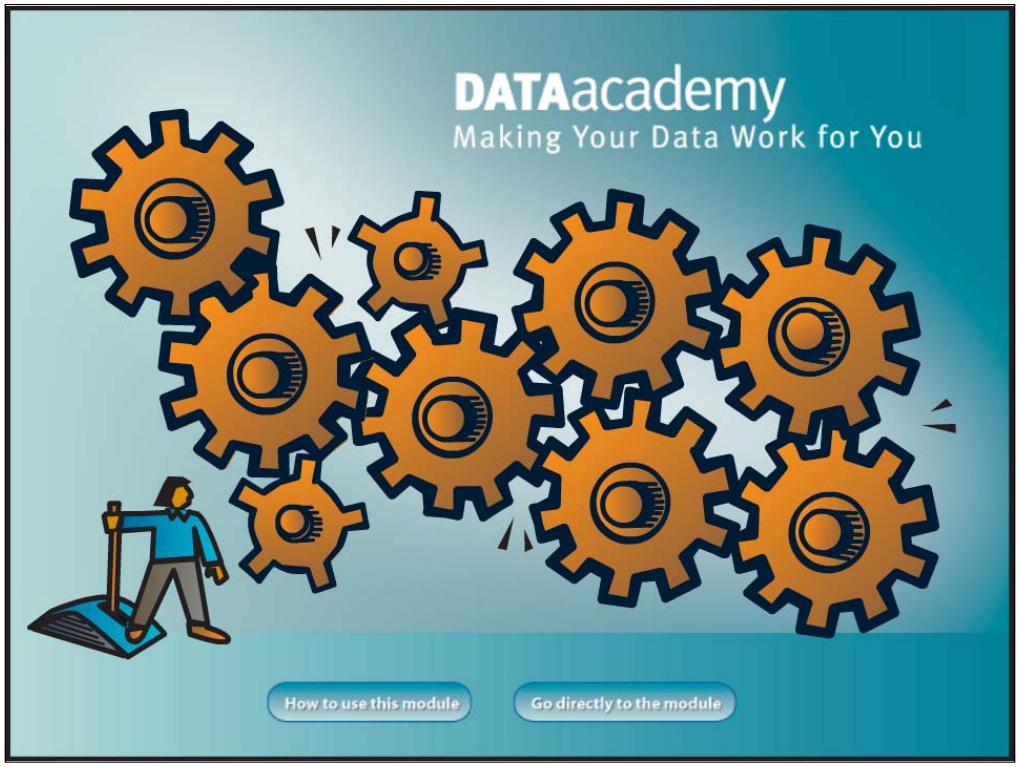
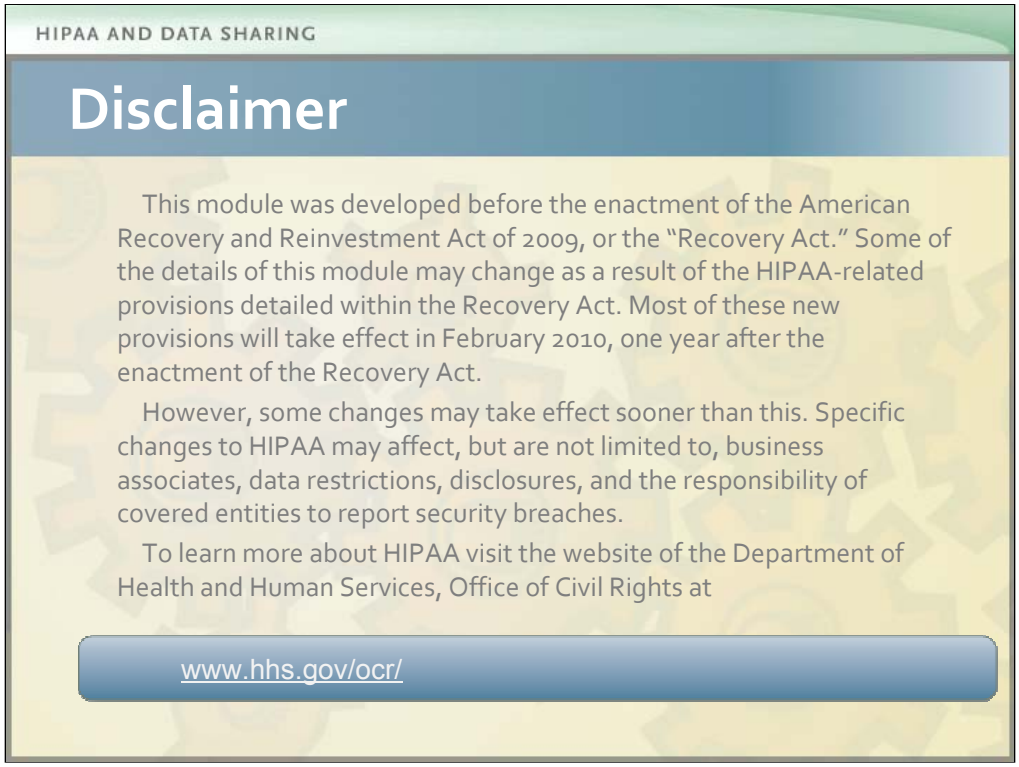


Welcome to Data Academy. Data Academy is a series of online training modules to help Ryan White Grantees be more proficient in collecting, storing, and sharing their data.

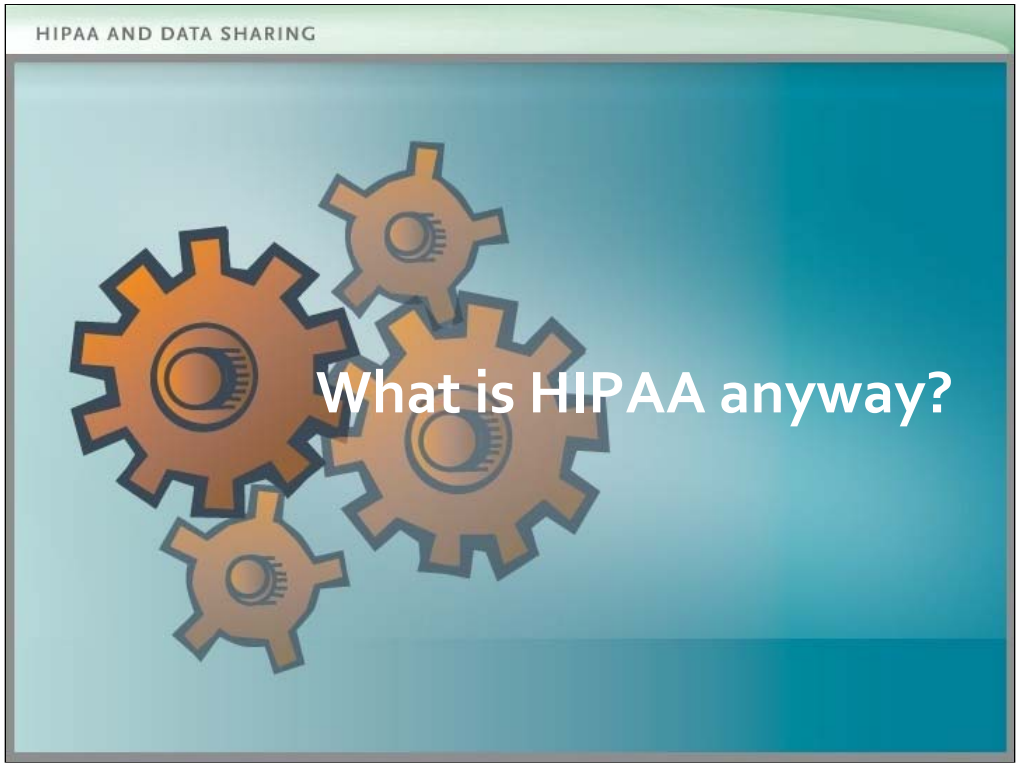
Let's get started with the module "HIPAA and Data Sharing."



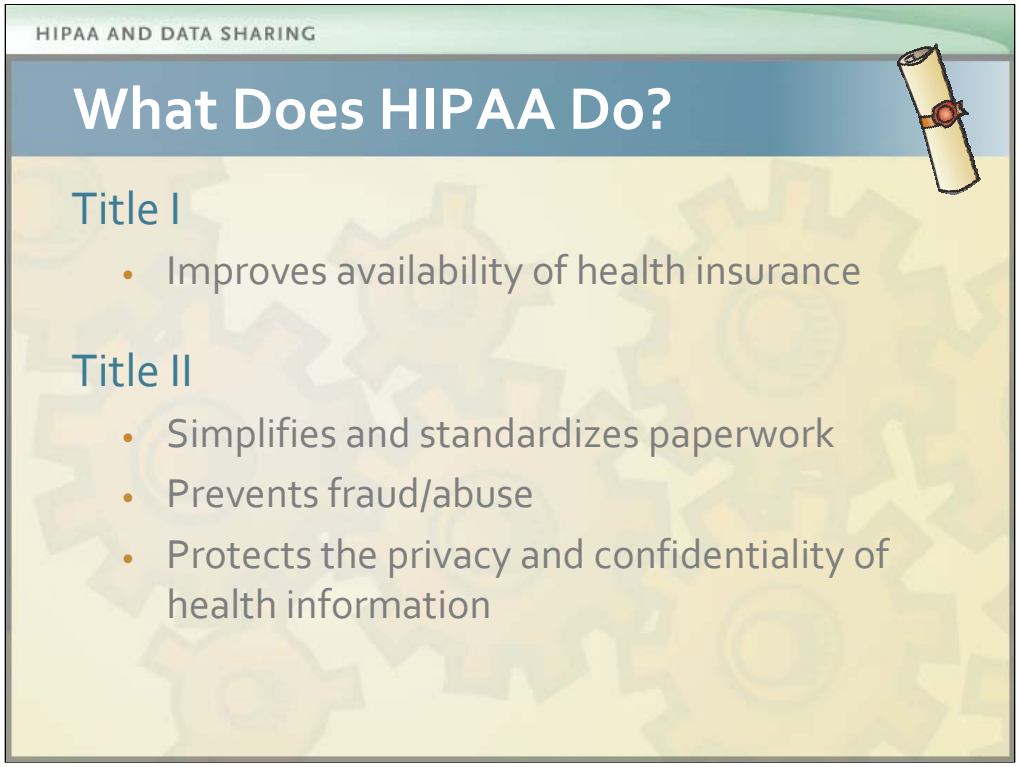
This module was developed before the enactment of the American Recovery and Reinvestment Act of 2009, or the "Recovery Act." Some of the details of this module may change as a result of the HIPAA-related provisions detailed within the Recovery Act. Most of these new provisions will take effect in February 2010, one year after the enactment of the Recovery Act.

However, some changes may take effect sooner than this. Specific changes to HIPAA may affect, but are not limited to, business associates, data restrictions, disclosures, and the responsibility of covered entities to report security breaches.

To learn more about HIPAA visit the website of the Department of Health and Human Services, Office of Civil Rights at www.hhs.gov/ocr

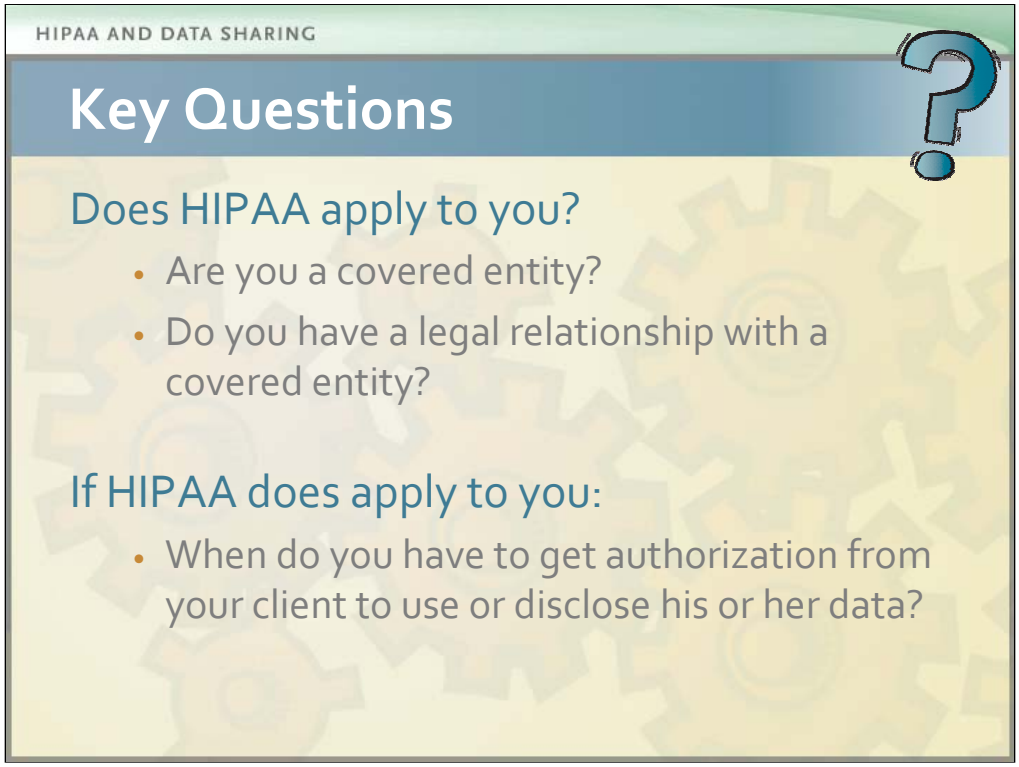


This module discusses HIPAA, the Health Insurance Portability and Accountability Act. This federal law governs how medical information can be collected and shared. It also establishes a national standard for protecting certain types of health information. HIPAA has major implications for the way health care organizations operate, especially how they collect, store, and share data about their patients.



While you've probably heard of HIPAA, there are often misconceptions about what it means and requires. HIPAA has two parts, Title I and Title II. Title I describes regulations about health insurance and covering individuals when they are between jobs. Title I improves the availability of health insurance. For this module, we're going to focus on Title II, the "simplification" of health information exchange that protects privacy and confidentiality of health information. Title II is sometimes called Administrative Simplification.

HIPAA is a national law, but individual states can enact additional laws that regulate how data is used and disclosed. HIPAA provides a floor, or a baseline level of protection. State laws can't take away any of the protections covered by HIPAA, but they can increase protection. Find out if there are any additional privacy and security laws in your state by seeking legal advice. You can also check your state's main government web site for information.



The main purpose of this module is to help you understand whether HIPAA does, or does not, apply to you, and under what circumstances you can share protected health information.

To do this, we're going to focus on two key questions.

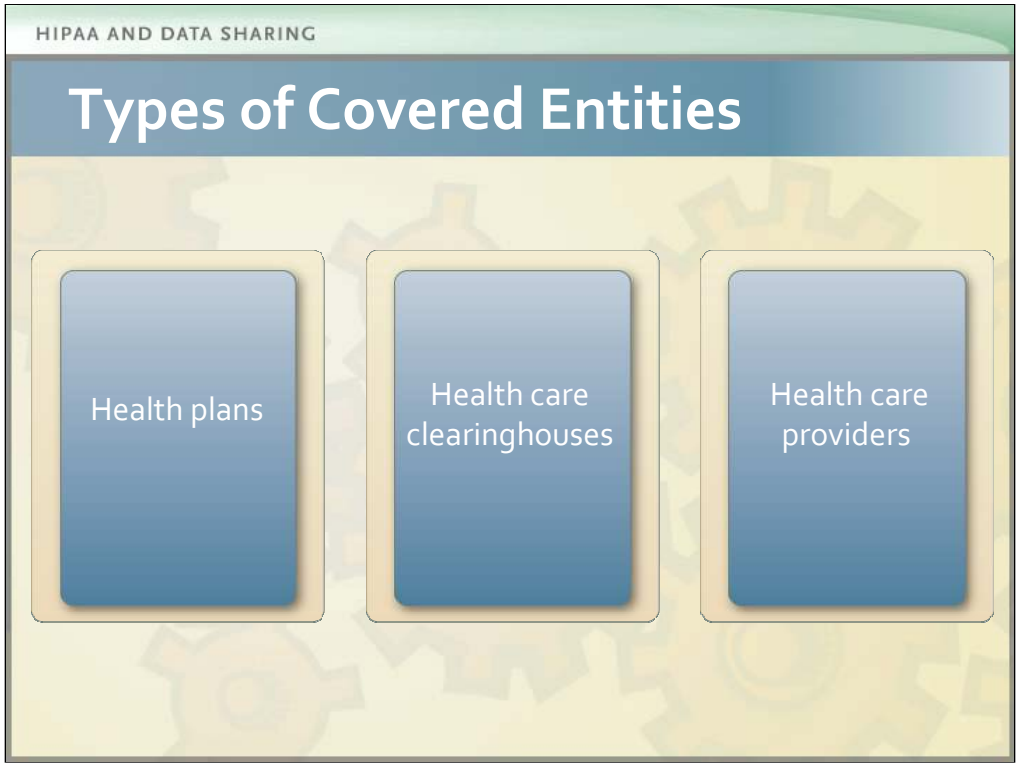
First, does HIPAA apply to you? To answer this question, we'll discuss whether or not your organization is a "covered entity", or has a legal relationship with a covered entity.

Second, if HIPAA does apply to you, when do you have to get authorization from your client to use, or disclose, his or her data?

Now we'll walk through the necessary steps to help you answer these key questions.

HIPAA only applies to you if your organization is a covered entity or, if you have a legal relationship with a covered entity.

The first question you need to answer is “are you a covered entity?”

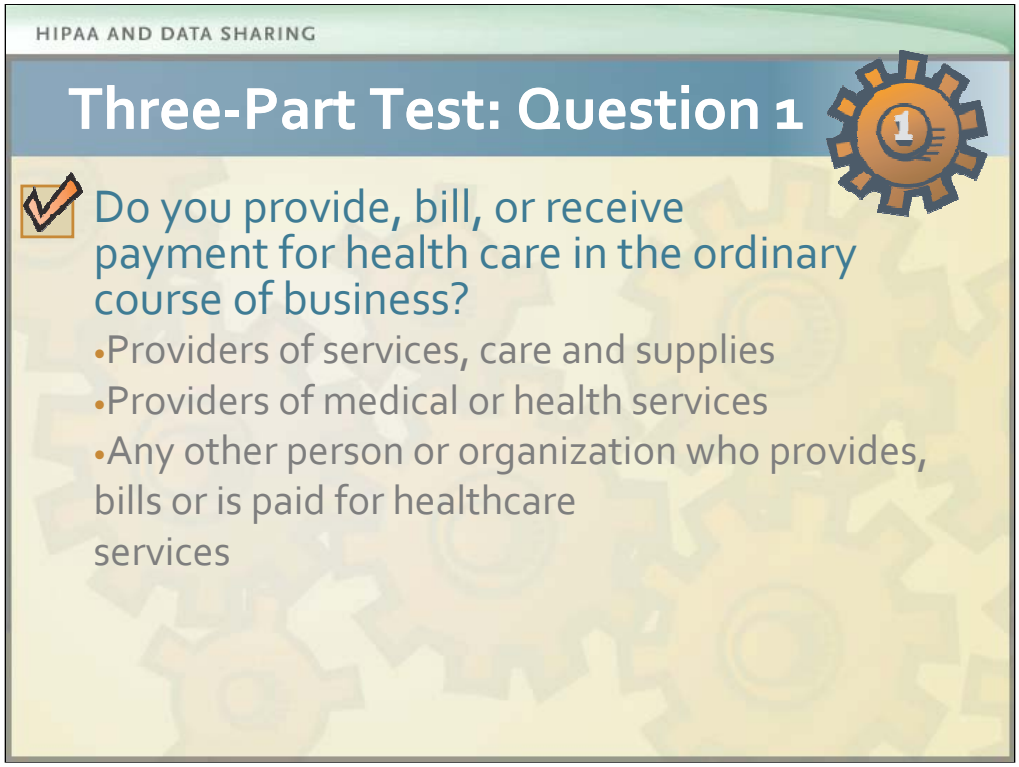


If your organization is a health plan or a health care clearinghouse, you're considered a covered entity and are always covered under HIPAA.

A health plan is any individual or group plan that provides or pays the cost of medical care. This includes private and public insurance payors.

A health care clearinghouse receives and processes non-standardized information from another entity into a standard format, or vice versa.

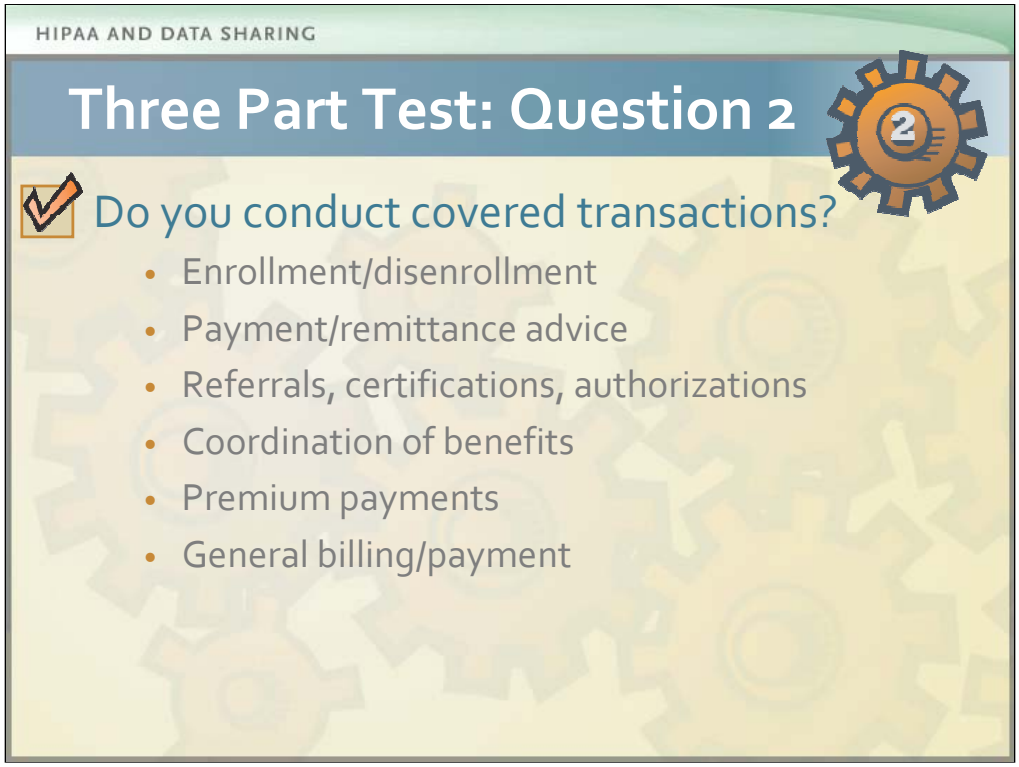
Health care providers are covered under HIPAA if they transmit health information electronically in connection with certain transactions. Many Ryan White care providers will fall into this category. We'll now go through a three-part test to determine whether or not you're covered as a health care provider. If you answer yes to all three questions in the three part test, you are a covered health care provider under HIPAA.



The first question is: do you provide, bill, or receive payment for health care in the ordinary course of business?

Health Care Providers include: All providers of services, care, and supplies, like hospitals and community health centers; Providers of medical or health services, like physicians and dentists, as defined by Medicare; and any other person or organization who provides, bills, or is paid for healthcare services.

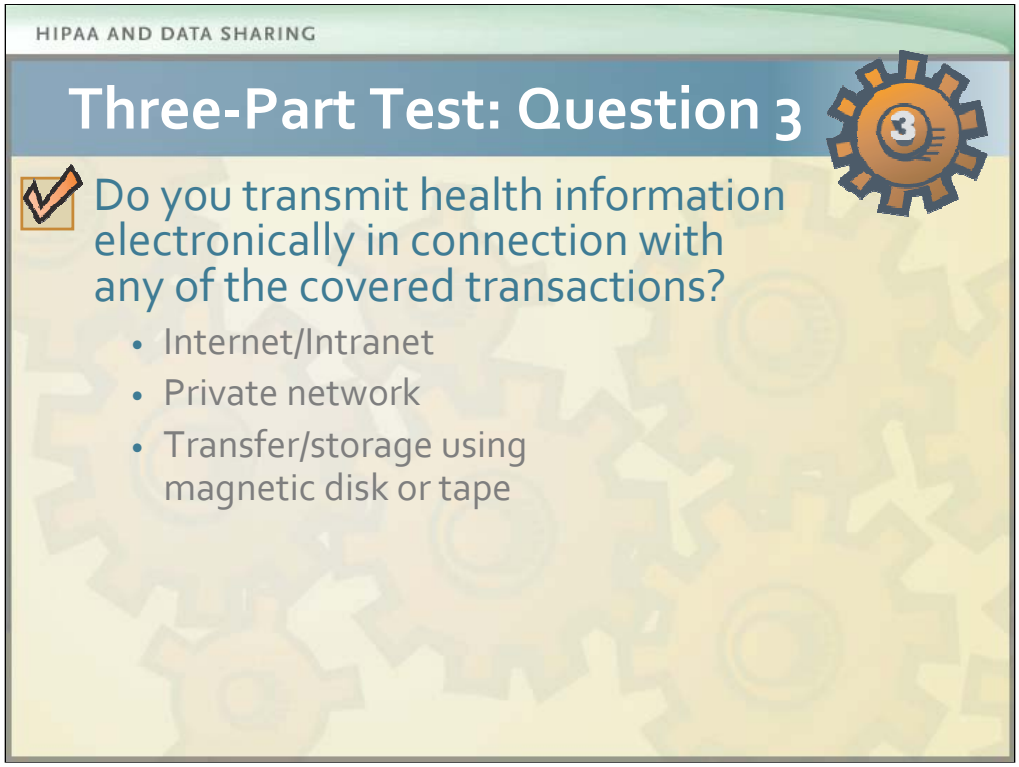
You can refer to the HIPAA legislation for a complete list of services.



The second question is: Do you conduct covered transactions? Covered transactions involve the sharing of certain health information for specific business purposes.

These include: the enrollment or disenrollment of individuals in an insurance plan; payment or remittance advice for healthcare services; referrals, certifications, or authorizations for healthcare services; coordination of benefits; premium payments for health insurance; and general billing and payment for health care services.

If your organization conducts one or more of these covered transactions listed here, or pays someone else to do so, for example, an outside billing service, then your answer to question two is “Yes.” If you don’t conduct any of these transactions, and don’t pay someone else to do so, your answer is “No.”

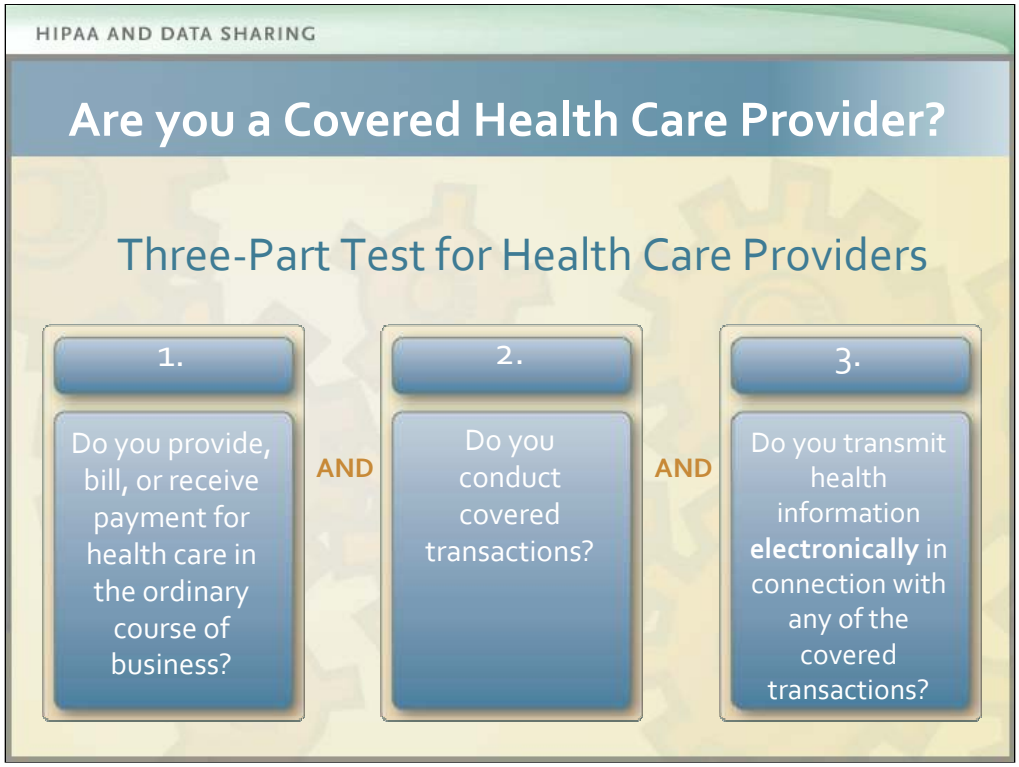


The third question is: do you transmit health information electronically for any of the covered transactions we just discussed?

If you share health information electronically in connection with a covered transaction, then your answer is “Yes”.

Electronic transmission methods include internet, intranet, private network, and transfer or storage using a magnetic disk or tape.

If all of your transactions are transmitted by paper, dedicated fax, or by phone, then your answer is “No”. However, most organizations transmit at least some health information electronically for one of the covered transactions.



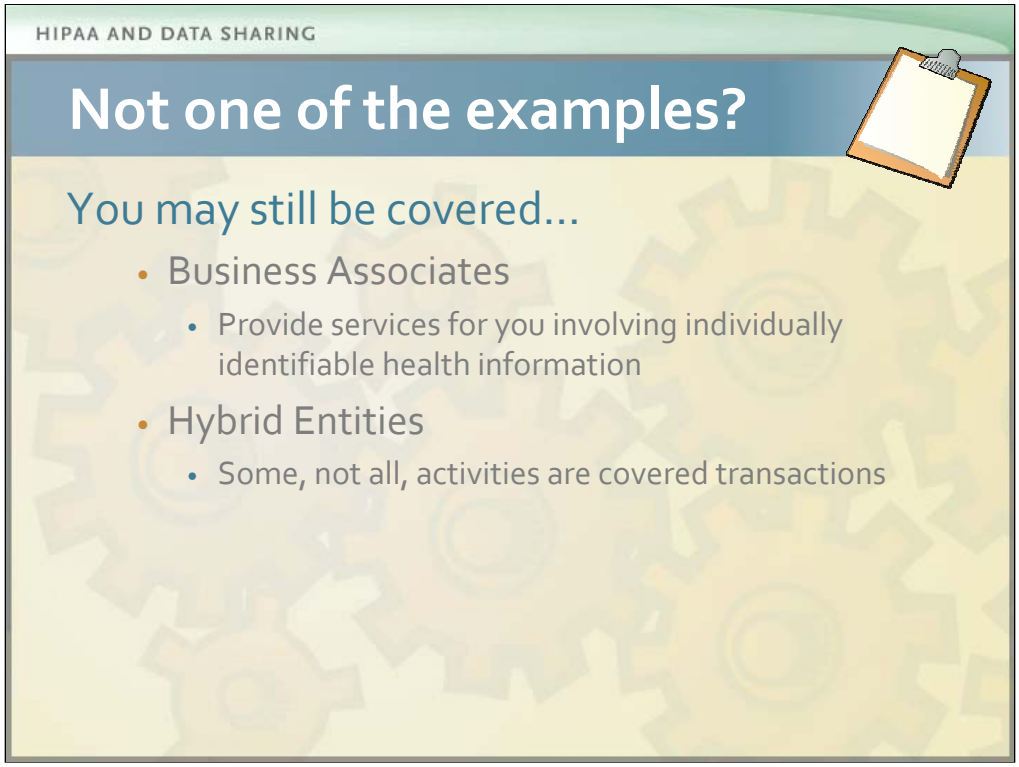
Now, let's review your answers to the three part test. To be covered under HIPAA, a health care provider must transmit health information electronically in connection with certain transactions.

First, do you provide, bill, or receive payment for health care in the ordinary course of business?

Second, do you conduct covered transactions?

Third, do you transmit health information electronically in connection with any covered transactions? Remember, if you only transmit health information by paper, phone, or fax, your answer to question three is "No."

If you answered yes to all three of these questions, you are a covered health care provider under HIPAA. This also means that you are a covered entity under HIPAA. As we discussed earlier, the three types of covered entities under HIPAA are health plans, health care clearinghouses, and health care providers. If you answered no to any of these questions, you are not a covered health care provider, but you may still be covered under HIPAA.

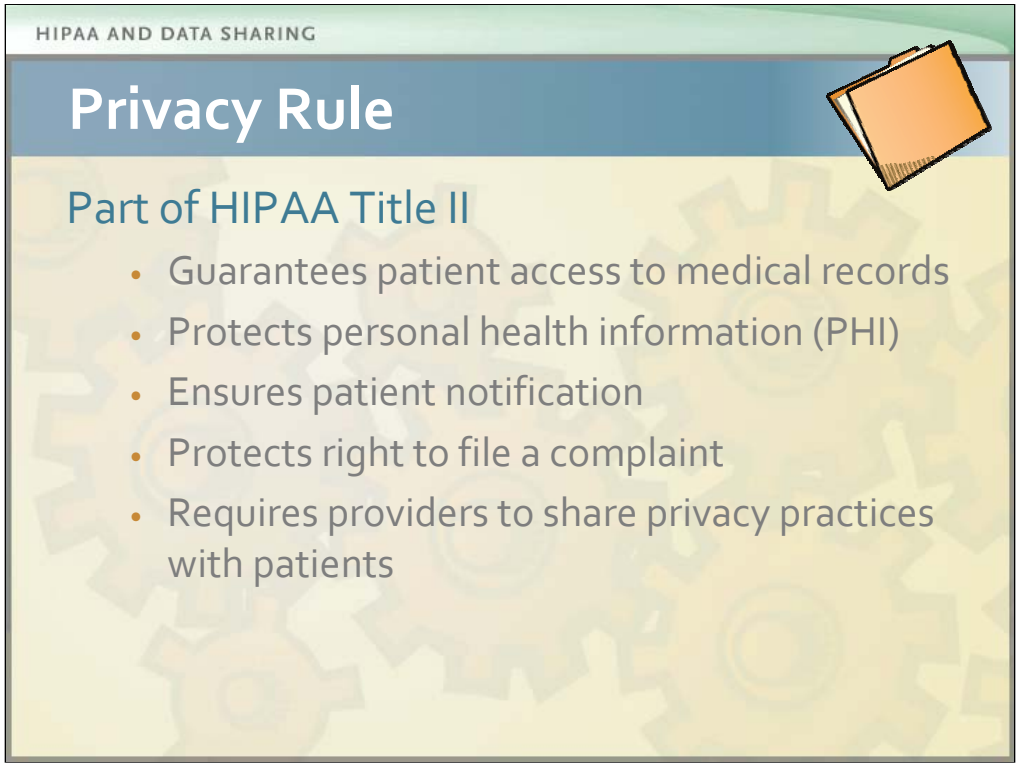


Even if you are not a covered entity, you may still be covered under HIPAA if you have a legal relationship with a covered entity. Two common examples are Business Associates and Hybrid Entities.

A business associate is a person or organization, separate from your organization, that provides services for you involving individually identifiable health information. These services most often involve claims, data analysis, and billing.

A hybrid entity is very similar to a covered entity. The only difference is that only some, but not all, of a hybrid entity's activities involve the sharing of individually identifiable health information. If all of an entity's activities involve covered transactions, they cannot be a hybrid entity – they are a covered entity.

Next we're going to discuss the HIPAA Privacy Rule. If you have determined that you are covered under HIPAA, then the HIPAA Privacy Rule applies to you.



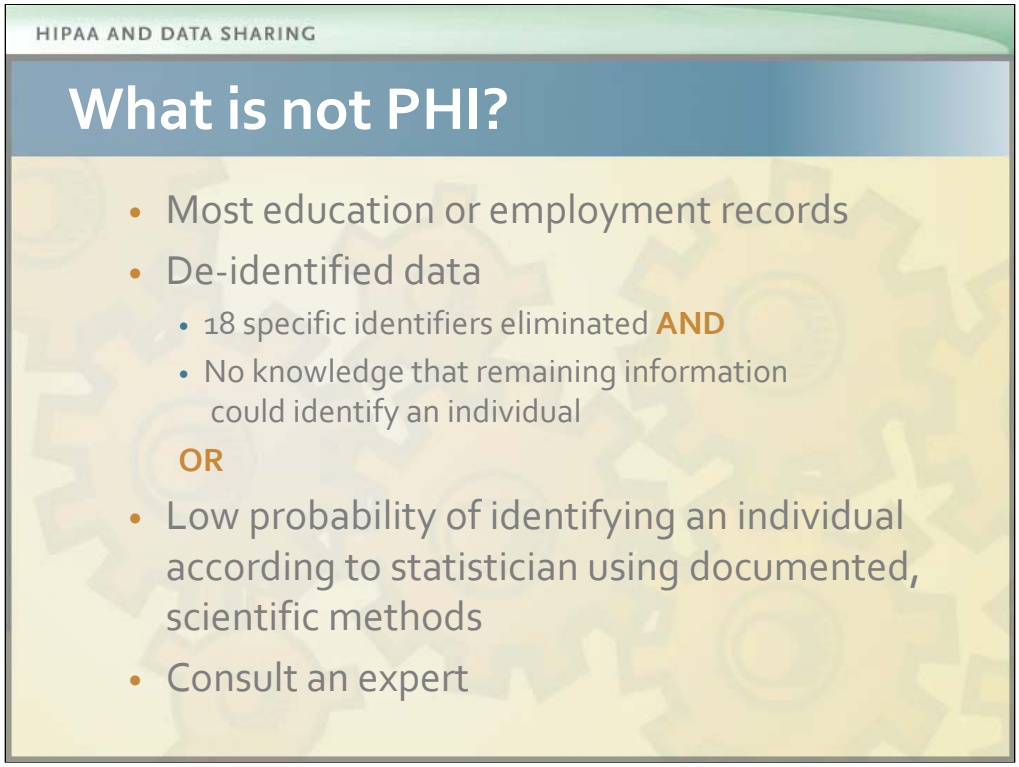
The "Privacy Rule" is a major part of HIPAA under Title II. This rule protects individual rights and provides guidance on how to do this.

The Privacy Rule guarantees patient access to medical records, protects personal health information, or PHI, ensures patient notification, protects the right to file a complaint, and requires health providers to provide patients with information on their privacy practices.

The Privacy Rule determines how you can use and disclose individually identifiable health information, which has to be treated differently than general health information.

Protected health information, or PHI, is individually identifiable health information that is transmitted or maintained in ANY form. This includes oral communication as well as paper and electronic methods.

Remember, if you are a covered entity, then HIPAA applies to all of your transactions. This includes electronic transactions, as well as transactions that are paper, phone, or fax-based.

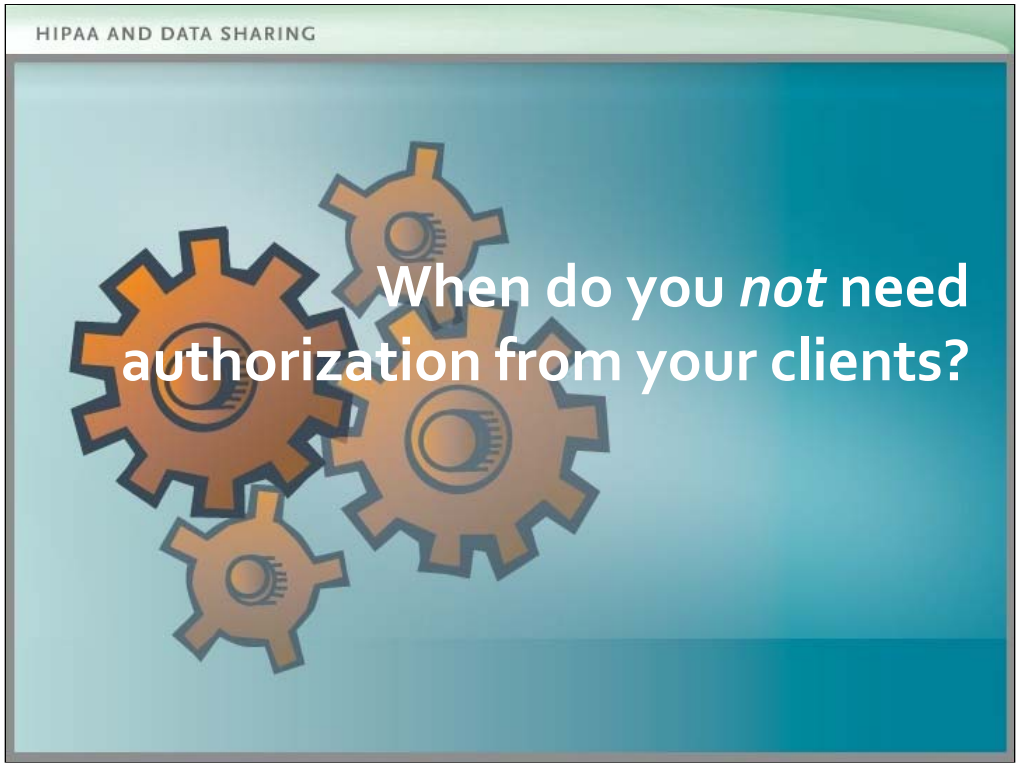


What is not considered protected health information? Most educational or employment records are not PHI. De-identified data are not considered PHI. There are two ways to de-identify your data.

The first way to do this is to remove certain identifiers for the individual, members of their family or household, and their employer. HIPAA lists 18 identifiers, including name, social security number, medical record number, and address. If any of these 18 identifiers are present in your data set, they must be removed. In addition, you must have no actual knowledge that the remaining information could be used to identify an individual.

The second way that information can be considered de-identified is by a qualified statistician. This person must be able to use documented, scientific methods to determine that there is a low probability of identifying an individual from the information in the dataset. Keep in mind that removing obvious identifying variables, like a client's name or date of birth, may not be sufficient to de-identify your data. Depending on the size and the content of the dataset, these variables could still be used alone or in combination with other variables to identify an individual.

Determining whether or not health information is protected depends on a lot of different things. It's important that you consult an expert to make sure you're complying with HIPAA standards.



So far in this module you've determined whether or not HIPAA applies to you, and you know what kinds of health information need to be protected.

Now let's talk about getting your clients' authorization to use and disclose their data.

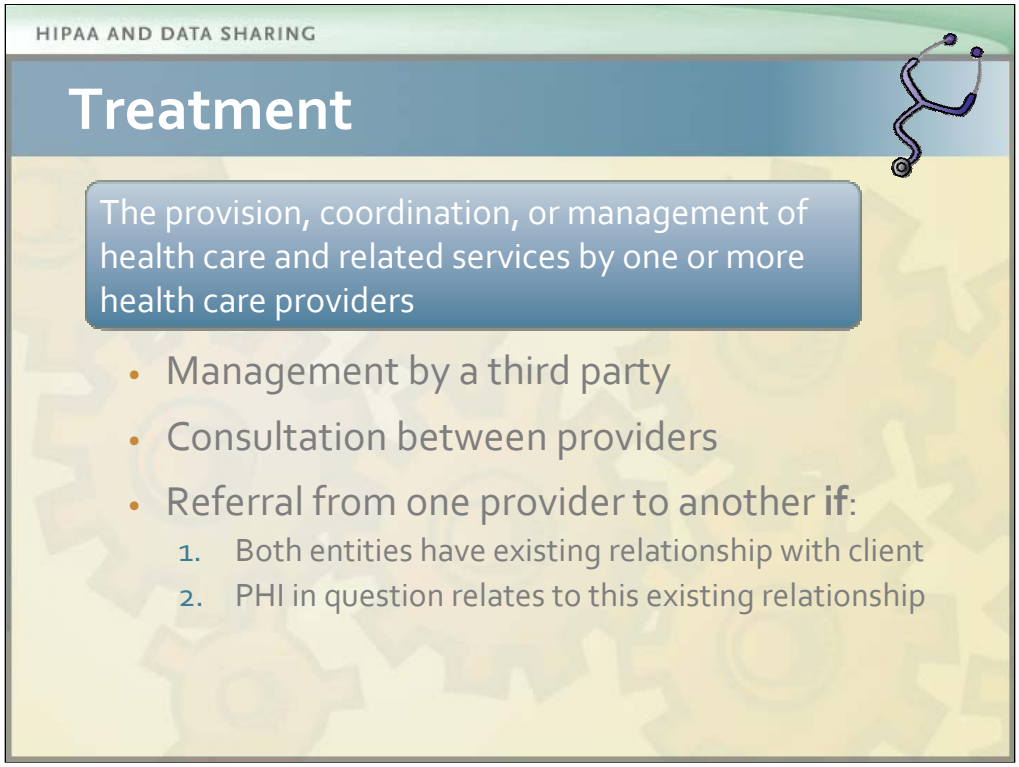
First, when do you not need authorization from your clients?

There are two situations where you are required to disclose PHI and do not need to get specific authorization from your client. These are known as “Required Disclosures.”

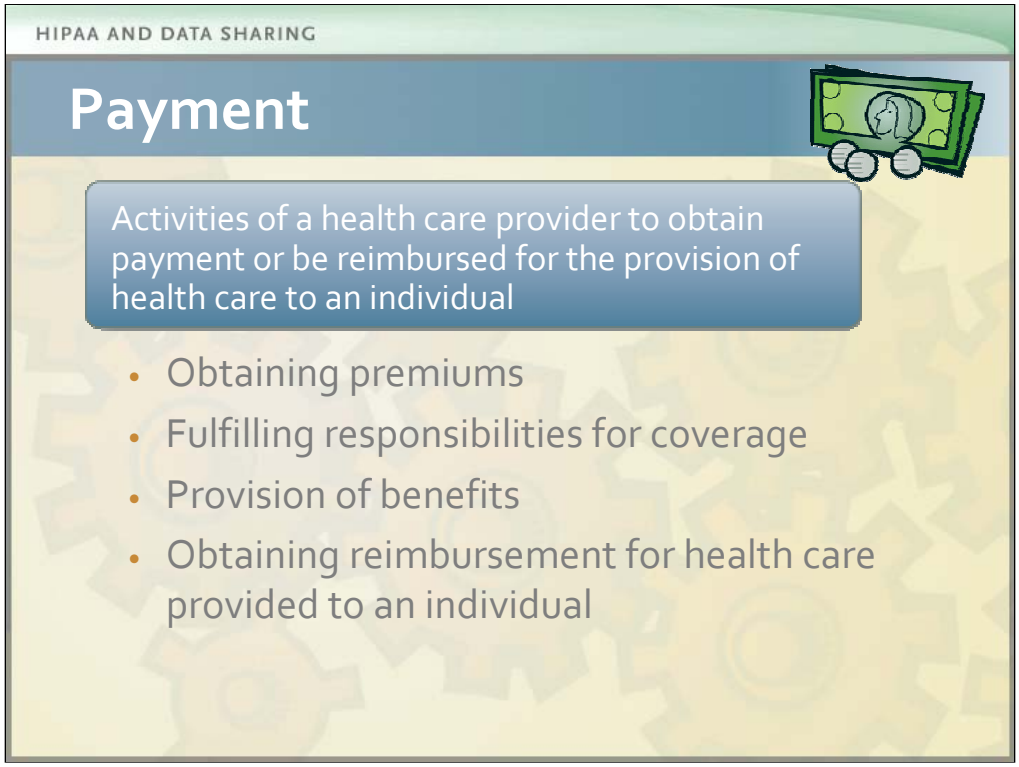
The first required disclosure is to the individual who is the subject of the information, or the “subject individual.” A common example would be a patient who requests access to his or her own health information.

The second required disclosure is to the Department of Health and Human Services. The purpose of this is to determine whether or not your organization is compliant with the Privacy Rule standards. There are other situations where you are permitted, but not required, to use and disclose data without the client’s authorization. These are called “permissive disclosures.” Let’s talk about these next.

There are three situations where HIPAA allows you to use and disclose data without your client's authorization. Authorization is not required for: Treatment, payment, or health care operations; Uses and disclosures for which individuals can verbally agree or object; and For public interest and benefit purposes. Again, use and disclosure of data for these purposes is permitted under HIPAA. We will now explain each of these situations in detail.



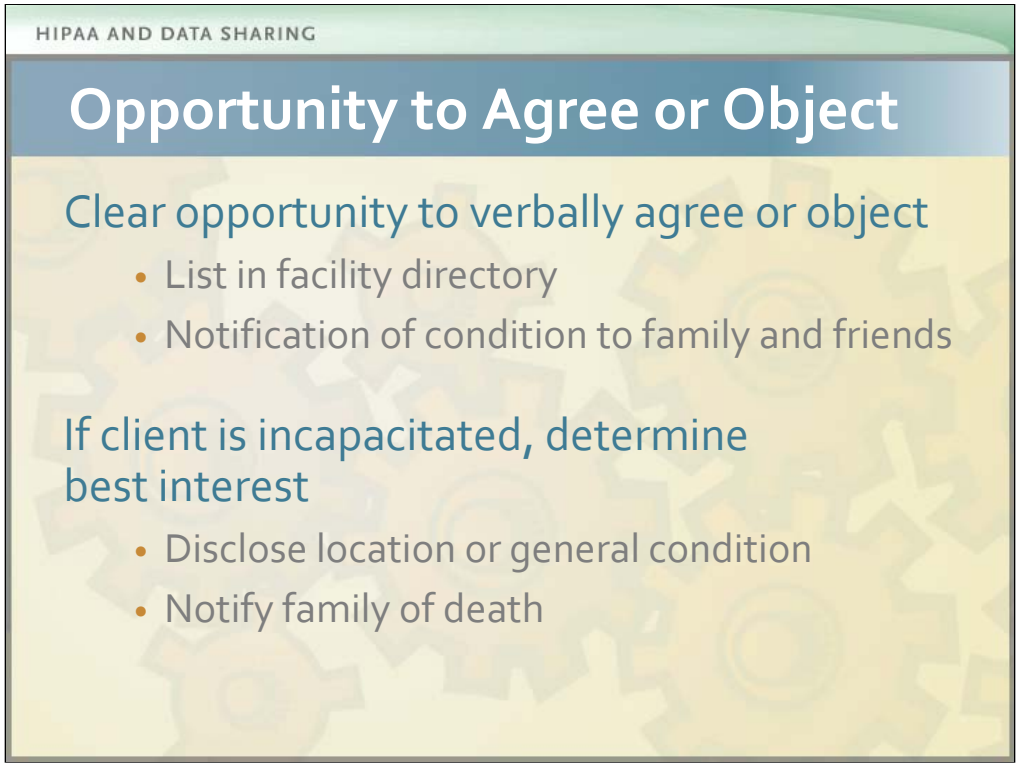
The first situation where client authorization is not required is for treatment, payment, or health care operations. Treatment includes the provision, coordination, or management of health care and related services by one or more health care providers. This includes: coordination of health care by a provider with a third party, consultation between providers, and a referral from one provider to another. Referrals are a little confusing and it may be best to seek legal advice. In general, you are permitted to share health information between covered entities without authorization from your client under the following two conditions: First, both entities must have an existing relationship with the individual. Second, the protected health information (or PHI) in question must pertain to this relationship.



Payment refers to the activities conducted by a health plan including: obtaining premiums, fulfilling responsibilities for coverage, and provision of benefits under the health plan to an individual. Payment also includes activities by a health care provider or a health plan to obtain or provide reimbursement for health care provided to an individual.

Health Care Operations are activities that are necessary to maintain and monitor the operations of your institution. Health Care Operations include, but are not limited to: quality assessment and improvement, performance reviews, and resolution of internal grievances.

If you have questions about a specific activity and whether or not it is covered, you can refer to the HIPAA legislation directly, or seek legal advice.



The second permissive disclosure situation includes circumstances where you are permitted to gain informal permission from your client, by clearly giving them the chance to verbally agree or object.

This could be as simple as asking someone if they wish to be listed in a facility directory. Another example is when a client agrees that their health information can be shared with specific family members or friends.

If a client is incapacitated then you, the covered entity, are permitted to determine the best interest of the individual. For example, you can disclose the location or the general condition of the patient, and you can notify family members in the case of death.

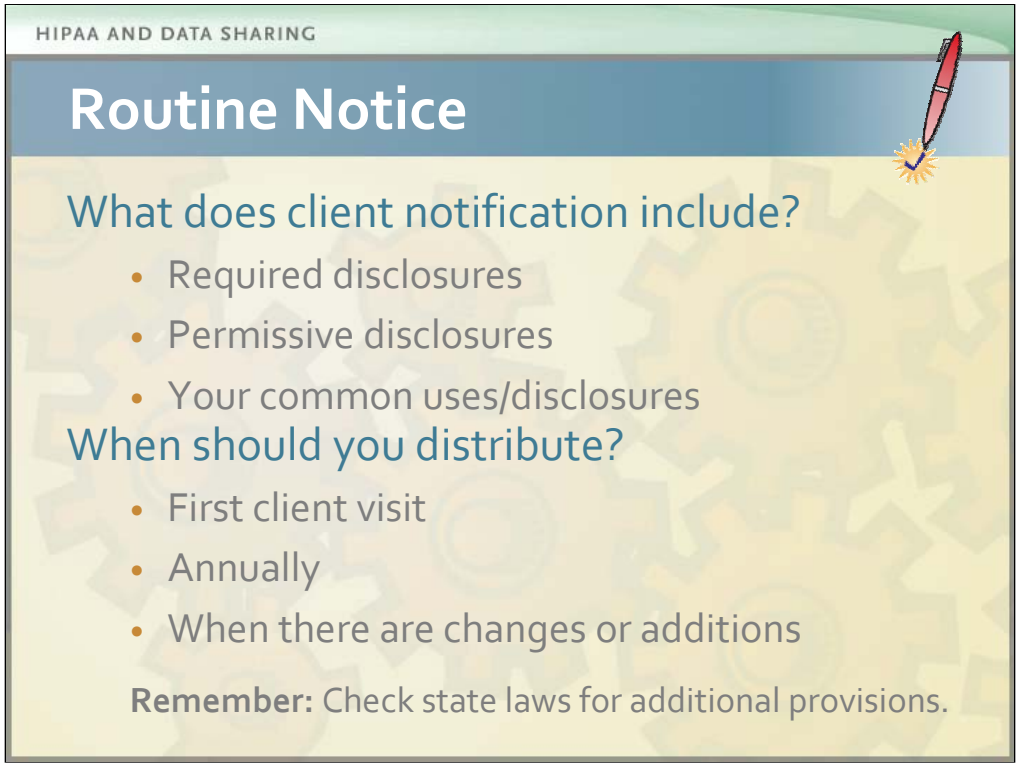
The third permissive disclosure situation covers public interest and benefit purposes. There are 12 identified national priority activities, but we are going to only review the three activities most relevant to Ryan White providers.

First, if disclosure is required by law, you don't need authorization from your client. Examples of this might include court order or law enforcement purposes.

Second, you don't need client authorization for specific health oversight activities as defined by HIPAA. An example would be a government investigation of a benefit program like Medicare.

Third, client authorization is not required to disclose personal health information to public health authorities for certain public health activities such as contact tracing or disease reporting.

Other examples that do not require authorization to use or disclose PHI include the facilitation of organ donation, releasing information in the case of death to a medical examiner or coroner, and worker's compensation claims.

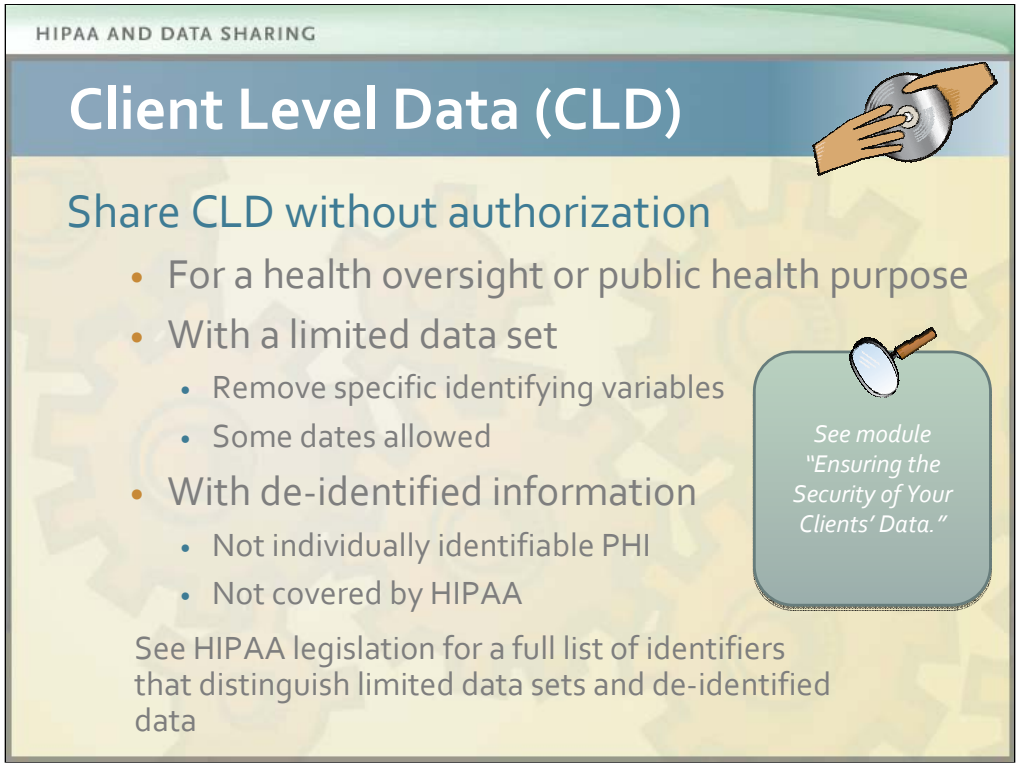


While you are permitted to disclose this information without client authorization, you must provide notice to clients explaining how their protected health information will be used and disclosed.

In this routine notice, you should describe the required and permissive disclosures in the Privacy Rule. This notice should also include all general and routine uses and disclosures of PHI at your organization.

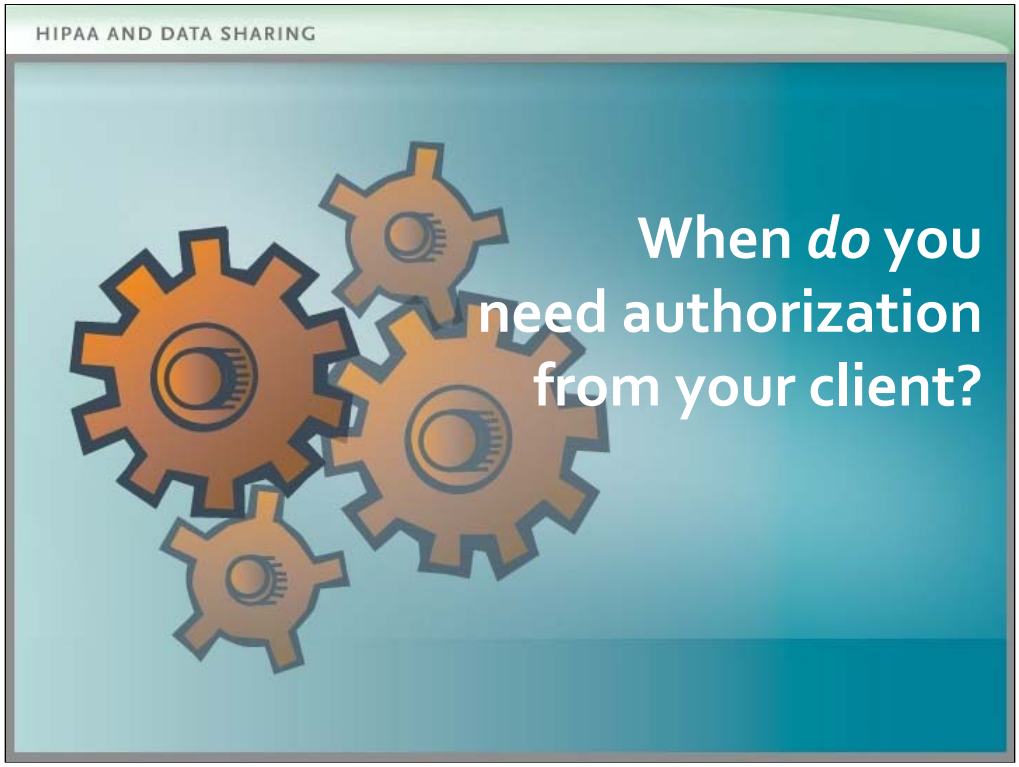
Notice should be distributed to the client: at their first visit to your organization, annually, and when any uses and disclosures are revised or added.

Remember that you should always check your own state's laws for additional provisions or disclosures.

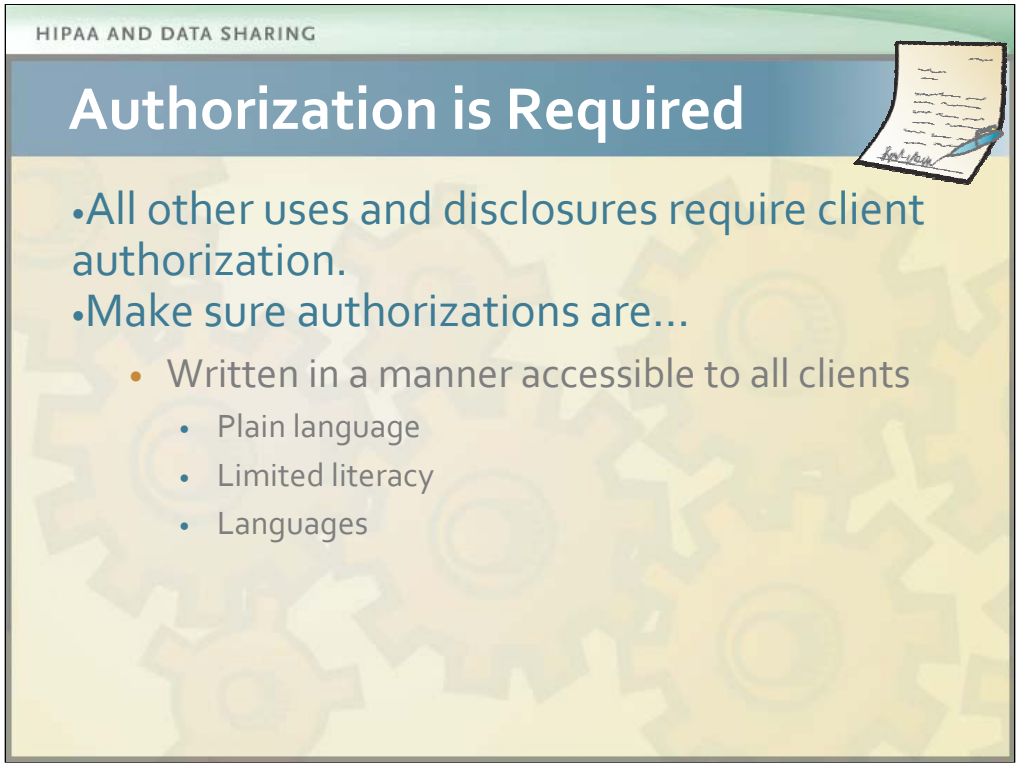


One of the biggest concerns about authorization and protected health information is what to do about client-level data. There are several ways you are allowed to use and disclose client-level data without authorization from individual clients. First, in the case of health oversight, you can share individual client data in a limited data-set. A limited data-set has specific variables removed that could identify the individual, or their relatives, employers, or household members. Also, de-identified data can be shared because it is not individually identifiable. Therefore, it is not considered protected health information and is not covered by HIPAA. The difference between a limited data-set and de-identified data is the number of identifiers that have to be removed. As we discussed earlier, for data to be considered de-identified, you must remove all 18 identifiers outlined by HIPAA. A limited data set, like de-identified data, eliminates all personal identifiers. The main difference is that a limited data set allows for the inclusion of some dates and some geographic information, such as city and zip code. You are also allowed to use and disclose client level data for health over sight or public health purposes. This was just covered under the section on Permissive Disclosures.

To learn more about sharing client-level data, see our module on data security.



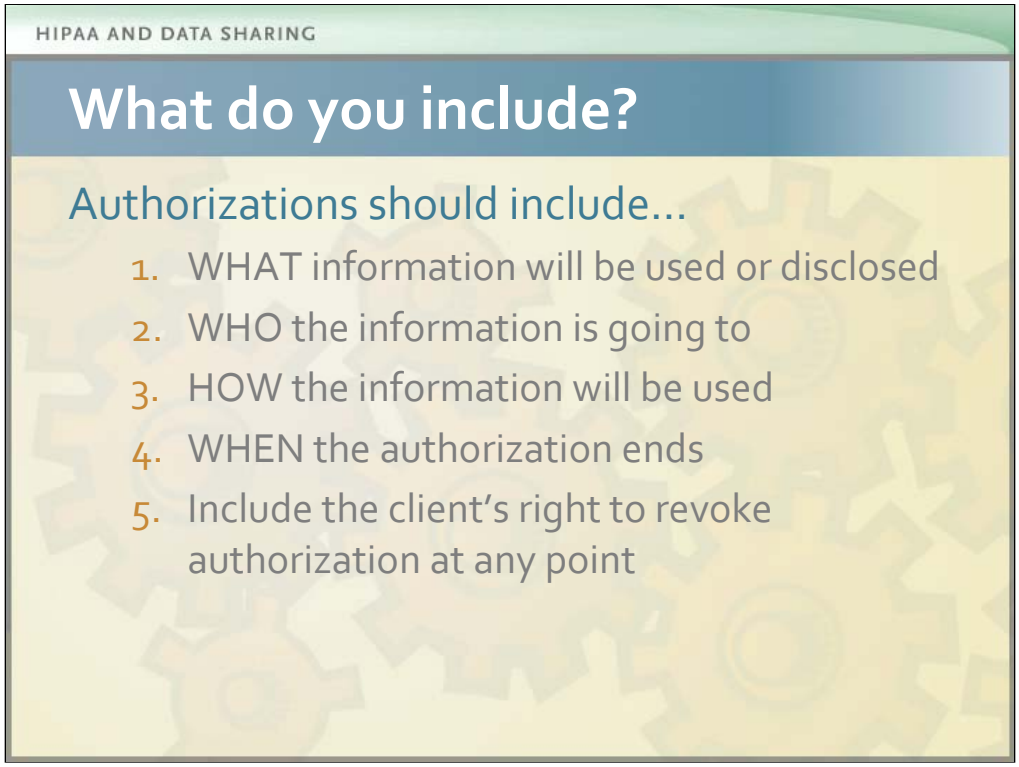
We've just covered when you don't have to obtain authorization from your clients. Next, we're going to discuss when you do have to get authorization from your clients to use and disclose their data.



If the activity doesn't fall into one of the categories that we've discussed in this module, you will need to obtain authorization from the client.

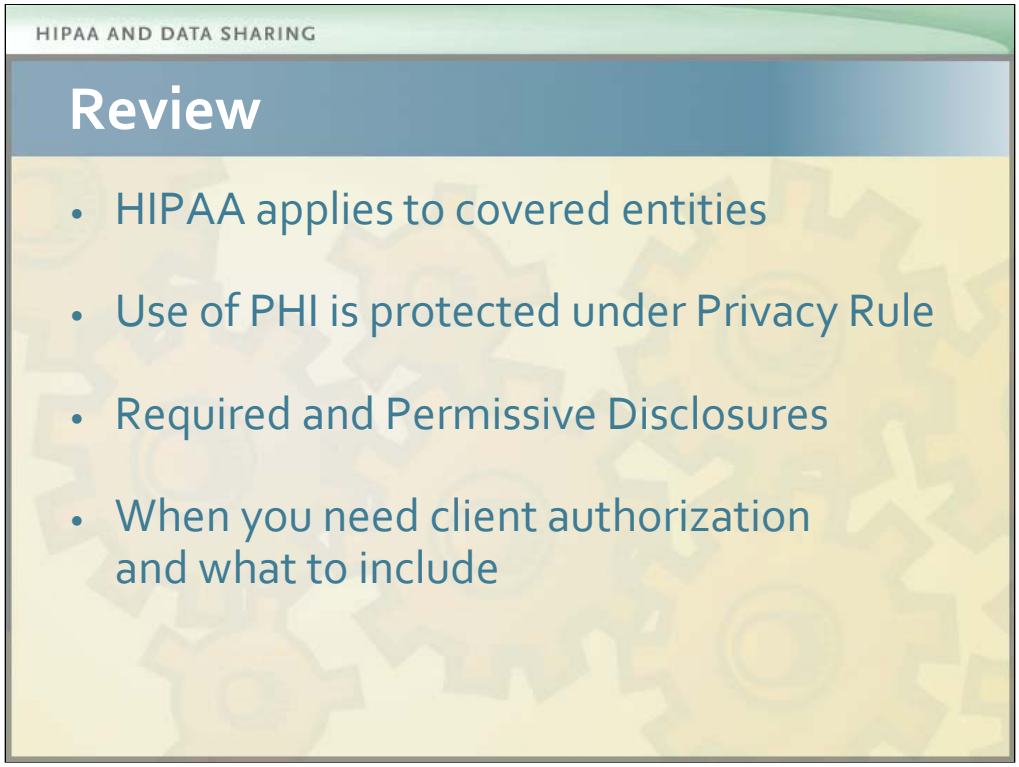
It is very important that authorization forms are written in a manner that is accessible and understandable to all clients. This includes several things: first, authorizations must be written in plain language and edited for clients with limited literacy. A common standard is for the literacy level to be between a sixth and eighth grade reading level. Also, although you do not have to provide materials in every language, you must be able to explain the authorization form to all non-English-speaking clients. This may include translating the document, or having staff members who are able to explain the contents to clients in their own languages.

It's important to note that none of these rules about authorization apply to substance abuse. There are separate federal regulations for this category.



So, you know when you need to obtain authorization from your clients to use and disclose their data, but what should be in the authorization?

The authorization form should describe: what information will be disclosed, who the information will be disclosed to, and how that information will be used. Finally, the authorization should contain an expiration date and describe the client's right to revoke their authorization at any time.



Let's review what we've learned.

First, we discussed what HIPAA is, and whether or not HIPAA applies to you. We did this by determining if you are a covered entity or have a legal relationship with a covered entity.

Second, we learned about the Privacy Rule. The privacy rule determines how you can use and disclose individually identifiable health information, or PHI.

Third, we discovered which situations you are required or permitted to use and disclose PHI without authorization and when you need to obtain authorization from your clients.

You have now reached the end of this module. We hope that you enjoyed the module and that it helped you build skills for collecting, reporting, using and sharing data. To view more Data Academy modules, visit the Data Academy home page. And to learn about other resources for Ryan White HIV/AIDS Program grantees, visit the TARGET Center website.