4Med™ Professional Training and Certifications

Meeting the HIPAA Training and Business Associate Requirements

Questions and Answers, with HIPAA Security Expert Mike Semel

	Questions	Answers
1	Is a Business Associate (BA) responsible for assuming a Covered Entity (CE) they work with is HIPAA Compliant? For example, the CE wants to delegate a piece of the business operations to a BA—does that BA have any obligation to do an assessment of the CE HIPAA compliance before sending back PHI to the CE? Or if a Business Associate Agreement (BAA) has been executed, is that sufficient?	There is no requirement for a Business Associate to assess the compliance of a Covered Entity. The Covered Entity has responsibility for the security of their patients' Protected Health Information (PHI.) The BA may send PHI to the CE per the terms of their agreements. However, a BA that becomes aware of a CE's HIPAA violations should bring it to their attention and is ultimately responsible for reporting the CE to OCR if they fail to correct the violations.
2	How can we get HIPAA certified?	Visit 4Medtraining for more information.
3	If an EMR/EHR vendor is a Business Associate, would the signed contract with said vendor be the BAA or would they need to sign an additional BAA?	It depends. You may either incorporate the terms of a BAA into a business contract, or have a stand-alone BAA. New BAAs must incorporate the language found in this recent guidance. If you have an agreement signed before January 25, 2013, it must be replaced with a new agreement including the new requirements by September 22, 2014.
4	Could you provide any guidance on recognized online training programs for small practices with 2 to 5 physicians?	4Med Approved offers HIPAA certification training for managers (qualifies for CEU's) and security officers, and HIPAA workforce certification for other staff members.
5	Where do we get the new language to update our BAAs?	New guidance is available here. An updated template of a BAA is included with the 4Medtraining CHSP course.
6	Are pharmacies Covered Entities or Business Associates?	They could be either, or neither. HIPAA Covered Entities must bill electronically for claims, or conduct other electronic transactions. So, if a pharmacy electronically bills health plans or Medicare they are a Covered Entity. There are some companies that provide outsourced pharmacy services to Covered Entities, and the Covered Entities bill electronically. These outsourced pharmacy services would be Business Associates of the Covered Entities. Finally, if a pharmacy only took cash, it would not be either a Covered Entity or Business Associate.
7	Do BAAs have to be Notarized?	No.
8	How does HIPAA affect small solo practices where	HIPAA policies are vague and do not list

	most things are done in-house?	specific procedures, in order to make them apply to the smallest 1-doctor practice as well as the largest health care provider or health plan that exists. Some regulations are Required and others are Addressable. You should be able to adapt HIPAA's requirements to any size organization.
9	What about when some insurance company or their associates demand patient records but they also send a note that patient authorization is not needed as this is HIPAA compliant?	Covered Entities include both providers and payers (insurance). Patient information may be shared between CEs for the purposes of treatment, payment, and healthcare operations. As a medical practice, you must provide your patients with a Notice of Privacy Practices (NPP) and get their written acknowledgment.
10	Is it OK to talk with pharmacies when they call for a refill or have a question about a prescription?	Yes, as long as you are confident that you are really talking to a pharmacy. If in doubt, verify their phone number and call back.
11	How about EHR companies and billing services and your merchant account companies?	EHR companies and billing services are Business Associates because they access patient info as part of their work. Merchant account companies (credit card processors) do not process patient data—just financial data—and are not Business Associates. Check with your merchant account company to determine your obligations to comply with the PCI DSS regulations.
12	Where do Coding and Reimbursement Compliance fit in the picture of a total Corporate Compliance Program?	Coding and reimbursements relate to Medicare and health plan payments, and are tied to civil and criminal penalties separate from HIPAA. It is estimated that over 70% of organizations that must comply with a regulation have to comply with multiple regulations. A Corporate Compliance Program would be the umbrella that oversees all compliance activities.
13	I just found out that a Business Associate has had an inappropriate disclosure but the new rules don't apply yet? The hospital is responsible for responding?	Yes. Until September, Business Associates will not be directly liable for data breaches. However, now and in the future, a BA is responsible for notifying their Covered Entity of any breaches, and the Covered Entity is responsible for responding to patients and the Office for Civil Rights.
14	Are cleaning crews required to have a BAA?	No. *From the US Dept. of Health & Human Services (HHS):* With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or

		disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.
15	Is a company that is a reinsurer for a health plan a CE or BA?	Neither. *From HHS:* Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. Each entity is acting on its own behalf when the health plan purchases the reinsurance benefits, and when the health plan submits a claim to a reinsurer and the reinsurer pays the claim. However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.
16	Our company obtains & stores provider information only. How does this affect our company?	If 'provider information' includes any Protected Health Information, then you are a Business Associate. Other types of data may be protected by other federal or state laws.
17	Will you offer a template for the Business Associate Agreement?	A BAA template is included in the 4Medtraining HIPAA training.
18	Is there a recognized HIPAA Certification?	The 4Medtraining HIPAA certification is certified by the 4Medapproved medical board. The course is also accredited for CEUs through ANCC and college credit by IACET.
19	Is a lab a CE or BA?	A CE. *From HHS:* A physician is not required to have a business associate contract with a laboratory as a condition of disclosing protected health information for the treatment of an individual. A hospital laboratory is not required to have a business associate contract to disclose protected health information to a reference laboratory for treatment of the individual.
20	If BAs have the same liability as CEs, can you confirm that they have to conduct regular risk assessments?	Yes they do. A risk analysis is the first requirement of HIPAA, and recent enforcement activities have cited non-existent or old risk assessments as compliance violations.
21	We are a clinical trial only research clinic—do not do insurance billing or charge the subjects—are we a HIPAA covered entity?	The National Institutes of Health (NIH) have issued guidance here.
22	Are there recommendations when choosing an	From a HIPAA standpoint, online backup

	outside backup system?	providers are Business Associates. Be sure your chosen provider will sign a BAA, implement a HIPAA compliance program, and ensure the compliance of any subcontractors (like data centers) they work with.
23	How does one become HIPAA compliant?	Implement written policies and procedures; train your workforce; perform HIPAA-compliant tasks; create evidence to protect your organization in an audit or data breach investigation. If you need assistance, contact 4Medapproved to discuss HIPAA compliance assessments and services.
24	I work for a technology Managed Service Provider (MSP) that has many medical clients as well as a Medical Billing company that is a sister company. As the Billing company, can we conduct the HIPAA audits and Risk Analysis for the IT side med clients as well as work on getting their compliance set up for them or would that be a conflict of interest?	This should not be a conflict of interest. Unlike Sarbanes-Oxley and other regulations that require independence to ensure objectivity and transparency, HIPAA has no specific requirements that would prohibit you from performing the services you described.
25	What are the implications for entities that have agreements for training students?	It depends on what role you play in the training. For example, Hospital A provides training for Hospital B's students. Hospital A would be a Business Associate of Hospital B if 'A' reviews 'B's patient records to evaluate the students. A BAA would be required. If you are a training company that comes in contact with patient data in the course of your work, you are a BA.
26	We have reps from our implant companies who access our patients' x-rays in order to template the implant size. Do I need a BA agreement with the company? In the past they have provided us documentation of HIPAA training but would not sign a business associate agreement.	If the medical device company bills for health care, then it is a Covered Entity. If its products fall under FDA jurisdiction you may share information without a patient's authorization. More details here.
27	I recently read an article that stated if a patient requests information via email and you notify them your email is not secure, you can send it provided they acknowledge they know you are sending it over a non-secure method.	You should be using a secure e-mail system to send any patient data because of the risks that unsecure systems can be easily breached and you could be responsible for large penalties and fines. The HIPAA Omnibus Final Rule says that if the patient asks you to send protected information to THEIR unsecure e-mail address, that you should inform them of the risks and get their authorization to do it anyway.
28	Are couriers for labs Business Associates because they pick up the specimen, verify patient info, and transport from location to location before	The labs are Covered Entities, and they may treat their couriers as members of their workforce, or have Business Associate

	returning to an actual lab?	Agreements with them. Unlike the Postal Service that blindly transports patient data, the couriers you describe access patient data as part of their work.
29	As a small wellness facility, we send diagnostic tests out to third-party labs by UPS etc., would they be considered business associates? Also, we have an agreement with a local lab for a courier service. It is for a medical facility—however, would those couriers be considered BAs?	UPS is a conduit and is not a Business Associate. See the previous question for information about the courier. It depends on whether they access protected data or just move packages.
30	If you use a Cloud-based accounting system, which uploads your bank checking info, and you write checks to patients as refunds which include their names and addresses, do you need to inform the patients you may place their info into a Cloud accounting and do you need a BA agreement with the Cloud based company?	As long as no information about the patient's treatment or diagnosis is entered into the accounting system then the Cloud provider is not a Business Associate. You only need a BAA if PHI is stored online.
31	Would you need a BA with an online scheduling system—where someone logs in to a website and schedules appointments with any doctor- (by name)? (like ZocDoc)	I don't believe so, because the patients are sharing their own information; it is not coming from a Covered Entity. There was a penalty in 2012 for a practice that used an online calendar to schedule patient visits and included the patient's name and treatment. Check with the scheduling system provider to be sure.
32	We log in remotely to our practice management system on the days the doctor isn't in so we can continue working—making appointments, answering questions. Is this a violation? Do we need a BAA with logmein or gotomypc?	Neither LogMeIn nor GoToMyPC transfers any electronic Protected Health Information through their systems; they link you to a host system you remotely control. This alone would mean that you do not need a BAA. However, if you have a problem and need support, and they open a remote session to help you connect, they are likely to see patient data and that would make them a Business Associate. You should contact them to ask if they will sign a BAA. FYI, LogMeIn offers guidance on how they can help you comply with HIPAA here.
33	If you have a file clerk that her job is just to file documentation in patient records, is it okay for her to read everything prior to filing them. I say no, but our General Manager says it is fine. I say she has no reason to be reading documentation, because she does not have a need to know any of the information.	HIPAA has a "Minimum Necessary" requirement that prohibits snooping in records unless you have a valid need-to-know reason (treatment, payment, etc.). If the clerk has no reason to read "everything" for filing purposes, then this is prohibited snooping. If your General Manager believes the clerk should be reading "everything," it would be best to document the reasons as part of the

		clerk's job description to protect your practice against a data breach allegation.
34	We are a physician service that only goes to Nursing Homes. Are we a business associate or are we a Covered Entity?	Assuming you are electronically billing Medicare and/or other health plans, you are a Covered Entity. The Centers for Medicare & Medicaid Services (CMS) has a website entitled Are You A Covered Entity? with more information.
35	Who has the right to see the compliance records? That is, can any patient demand to be shown that the med office is compliant?	Patients must receive a Notice of Privacy Practices from their healthcare provider and health plan. They do not have the right to audit a practice's compliance, but they are encouraged to file complaints if they believe there is non-compliance.
36	Is an IT company responsible if med office staff allows a breach? If patient covered info is visible on monitor or if paper chart is left where others can/have viewed it?	Business Associates are generally not responsible for breaches caused by Covered Entities, unless their actions (or negligence) created the circumstances for the breach.
37	If you use credit card machines to collect payments from patients, is the vendor you obtained the machine from a BA? Are there others involved in this process we should consider? Also, if the machine is showing the entire Social Security Number (SSN) I would assume internally this would not be a breach? If yes to this, is there concern with the information being transmitted via a phone line? Other issues to consider?	Credit card machines that just swipe card information do not collect any Protected Health Information. I have never heard of one that displays an entire SSN (which is protected by other federal and state privacy laws). Check with your payment card processor to ask about your PCI DSS compliance requirements.
38	Do all employees i.e. field representatives of an outsourced ROI Business Associate dealing with patient data directly have to be HIPAA certified?	HIPAA certification is not required, but your workforce must be trained prior to gaining access to any patient data and records should be kept as proof for an audit or data breach investigation. Retraining should occur at least annually.
39	For auditors coming in from the insurance companies to a provider's office, do you need a separate BA agreement? Do you need BA for insurance companies that would cover all employees?	Healthcare providers and insurance companies are all Covered Entities, so BAAs are not necessary.
40	How do I inform a patient if we believe their information has been breached?	Data Breach Notification guidance is available here.
41	Are the banks/credit card companies considered BAs, as they do receive checks/cc for deposit that a patient has written? The checks/credit cards have PHI.	No. *From HHS:* When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for

		payment for health care or health plan premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity.
42	How does the BAA work for data swapped between two Covered Entities i.e. physician office calling in the prescription into a pharmacy?	A BAA is not requires as both are Covered Entities sharing information for the treatment of a patient.
43	I am interested in HIPAA Certification, but fear the unregulated environment that these are offered in. Are there programs that you would recommend? Will HHS or OCR ever sanction a specific program?	I have had a HIPAA certification for 10 years and it has served me well. I admit I am biased, but check out the HIPAA certification training from 4Medapproved. I do not believe that HHS or OCR will ever sanction a program. They are focused on protecting patient privacy, not evaluating training.
44	Does HIPAA cover Internet Service Providers (ISP) who link practices to the cloud? Do ISPs have to be informed and sign that they have been informed of HIPAA by each entity using their ISP?	ISPs are considered "conduits" if they just transport data and are not covered by HIPAA as Business Associates. However, if they provide you with online storage or backup services for patient data, then they are Business Associates.
45	How much due diligence do you have to do to confirm your Business Associate is HIPAA compliant? What if they say they are and you don't check. Are you liable?	Yes, you can be liable. In today's regulatory environment you need to consider your risks of penalties and million-dollar-plus fines and notification costs before you share data and then find out your Business Associate breached thousands of patient records. Check out the Omnicell breach to see what can happen.
46	How do we address admitting department verifying patient information without committing a violation in a paperless system?	Admitting departments need to be designed to ensure patient privacy. Your admitting clerks should be aware of anyone nearby who is not authorized to hear the patient's info, and stop the conversation until it can be conducted privately.
47	I am a consultant who works on different healthcare program installations. I have responsibilities for management and oversight of projects that deal with patient or claim date; i.e. data conversion, but I do not have direct access to the data. Am I considered a Business Associate?	If you go on site to manage installations, and are likely to contact PHI, you are a Business Associate. If you do not go on site, and just manage and oversee implementation schedules or work tickets, you are not a BA.
48	Have there been any problems from discarded fax rolls?	Maybe I do not understand the question, but the fax rolls we discarded (before going to an electronic system) contained just a bit of blank paper or were down to the cardboard

		tube. If there is any PHI on the fax rolls then they should be shredded or burned.
49	Are surgical implant reps considered covered entities or business associates?	If the medical device company bills for health care, then it is a Covered Entity. If its products fall under FDA jurisdiction you may share information without a patient's authorization. More details here.