Compliance Bulletin

May 2013

*HIPAA Final Omnibus Rule Requirements and Impacts**

Effective March 26, 2013 and Compliance Deadline is September 23, 2013

	REQUIREMENT	IMPACT
1. Notice of Privacy Practices	Changes to notice of privacy practices.	Covered entities (CEs) must change the notice of privacy practices (NPP) to include: • Prohibition of sale of PHI • Duty to notify in case of a breach • Right to opt out of fundraising • Right to restrict disclosure for out-of-pocket payments • Limit on use of genetic information
2. Use and Disclosure of Protected Health Information (PHI)	New categories of PHI may be used or disclosed for fundraising	Healthcare organizations can better target fundraising efforts based on these categories.
	Strengthened opt-out-for fundraising	CEs may not make fundraising communications after opt-out, but may provide method of opting back in.
	CEs may combine "conditioned" and "unconditioned" authorizations for research to simplify authorization paperwork.	• The authorization must differentiate between these two portions. • Unconditioned authorization must be opted in.
	There is a new interpretation on authorization for future research.	Authorization may be used for future research, with notice to individuals.
	The Final Rule changes access to student immunization records.	CEs may release immunization records to schools without an authorization that meets HIPAA standards.
	Decedents' PHI under HIPAA protection for 50 years after death. Covered entities also have a greater	The Final Rule enables covered entities to continue communicating with relevant

Call the Care1st Hotline at 1-877-837-6057
Or the Care1st's Compliance Officer, Brooks Jones, at 323-889-6638
To report suspected and actual breach of Care1st members' protected health information (PHI)

THANK YOU FOR YOUR CONTINUED COMMITMENT IN COMPLIANCE

Whitepaper: *An Analysis of the Changes Impacting Healthcare Covered Entities and Business Associates by* ID Experts – Lincoln Center One, 10300 SW Greenburg Road, Suite 570, Portland, OR 97223. info@idexpertscorp.com

	flexibility to disclose PHI to persons involved in a decedent's care or payment.	family and friends after an individual's death.
	New definition of marketing includes remuneration from a third party for describing their product or service.	Covered entities must obtain authorization for third-party marketing.
	Genetic information is now considered PHI.	Health plans may not use or disclose genetic information for underwriting purposes.
3. Breach Notification	New definition of a breach replaces the "risk of harm" standard with the "probability" that Personal Health Information (PHI) has been compromised. The entity retains the burden of proof, however.	• Covered entities (CEs) and Business Associates (BAs) must conduct and document an objective risk assessment to determine probability and support the decision to notify or not notify. • Risk assessments must include steps to mitigate risks to PHI. • CEs and BAs are still required to "mitigate adverse consequences" and to notify individuals when the probability of PHI being compromised is not low. • Entities must update policies and procedures and retrain their workforce.
	The exception for limited data sets that did not contain birth dates or zip codes has been removed.	Entities must conduct risk assessments following all PHI privacy and security incidents.
	State and federal laws are more aligned.	More stringent state laws may be applied, as they are not contrary to federal law.
4. Business Associates	Expanded the definition of a business associate is one that creates, receives, maintains, or transmits PHI on behalf of a covered entity, as well as other specific types of organizations.	• "New" business associates have the same liability as existing BAs • They must bring business processes and systems into compliance with HIPAA rules. • CEs must enter into appropriate contracts with these new BAs.
	Subcontractors are now considered business associates and are bound by the same HIPAA privacy and security requirements.	• Subcontractors must bring business systems and processes into compliance with HIPAA privacy and security requirements. • BAs must revise contracts with subcontractors to reflect HIPAA requirements.
	Business Associate contracts must specify requirements for breach notification, electronic access to PHI, etc.	• BA contracts must specify compliance with the Breach Notification Rule. • If a CE designates HIPAA liability, the contract must specify BA compliance. • Contracts must specify to whom the BA

		provides electronic access to PHI. • One-year grandfathering may be available.
5. Increase Enforcement of Willful Neglect	The Office of Civil Rights (OCR) enforcement focuses on willful neglect, defined to be "conscious, intentional failure or reckless indifference."	OCR will: • Investigate all cases of possible willful neglect. • Impose a penalty on all violations of willful neglect.
6. Patient Rights	Restriction of disclosure for out-of-pocket payments.	CEs must agree to an individual's request to restrict disclosure to a health plan if the individual pays in full for a service or item.
	Copies of PHI to third parties must be authorized.	Authorization must be made in writing, and clearly identify the recipient and where to sent the copy.
	Electronic copies of PHI must be made available.	CEs must provide a readable electronic copy of PHI, rather than a hard copy, even it is not readily producible.

DEFINITIONS:

Covered Entity (CE) -