HIPAA Compliance Checklist

✓	Task
Breach Notification Policies:	
	Implement new compromise standard, discontinue use of the subjective harm standard
	Update policy to notify the Secretary no later than 60 days after the calendar year in which a breach affecting fewer than 500 individuals is *discovered.*
Fundraising Policies	
	Add categories of PHI that may be used or disclosed for fundraising Department of service Treating physician Outcome information Health insurance status
	Strengthened opt-out procedures
Research Policy	
	Authorization must clearly differentiate unconditional and conditional portions.
Immunization Records Policy	
	CE may release student immunization records to school without authorization IF required by state law AND written or oral agreement is documented.
Decedent Information Policies	
	CE may disclose PHI to persons involved in decedent's care or payment if not contrary to prior expressed preference
	PHI becomes public information 50 years after death
Marketing Policies	
	CE must obtain authorization for all all communications when financial remuneration is received for making communication from a third party whose product or service is being marketed
	Remuneration must be reasonable related to the cost of communication.
Sale of PHI Policies	
	CE cannot sell PHI without an authorization

	Authorization must specifically state that the disclosure will result in remuneration for making the disclosure
	Establish a “reasonable cost-based” fee for renumeration
Genetic Information Policies	
	Clarify that genetic information is health information
	CE may not disclose genetic information to a health plan for underwriting purposes
Business Associate Policies	
	Include language in the BAA that states the BA will comply with Breach Notification Rules
	Specify to whom BA provides electronic access
	If CE delegates HIPAA responsibility, must specify that BA will comply with HIPAA
Patient Rights Policies	
	CE must provide electronic copies of medical records to patient upon request
	Patients may request medical records to be sent to a person representative and be charged a reasonable cost-based fee for copies
	CE has a one-time extension of 30 days when records are kept offsite
	CE must honor requests to restrict disclosures to a health plan for services paid out-of-pocket in full, if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law
Changes to Notice of Privacy Practices	
	Prohibition on sale of PHI without authorization
	Duty to notify affected individuals of a breach of unsecured PHI
	Right to opt out of fundraising
	Right to restrict disclosure of PHI when paid out of pocket
	Limit on use of genetic information
Workforce Training	
	Update employees on new policies and procedures