Hospice Tool: Checklist of HIPAA Breach Action Steps

The following breaks down (i) what constitutes a "breach" of protected health information ("PHI") under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"), and (ii) action steps when a potential breach is discovered. Note, it is important to consult state privacy laws which could have different breach standards and requirements.

A BREACH IS:	"[T]he acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [HIPAA] which comprises the security or privacy of the [PHI]."[1]
BREACH EXCEPTIONS:	A "breach" does not include:[2] • Unintentional Acquisition, Access, Use or Disclosure – When done "by a workforce member or person acting under the authority of a covered entity or a business associate, [and if done] in good faith and within the scope of authority and does not result in further use or disclosure[.]" • Inadvertent Disclosure to Authorized Person – "Any inadvertent disclosure by a person who is authorized to access [PHI] at a covered entity or business associate to another person authorized to access [PHI] at the same covered entity or business associate . . . and the information received as a result of such disclosure is not further used or disclosed" as prohibited by HIPAA. • Inability to Retain Information – "A disclosure of [PHI] where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information."
4 FACTOR BREACH RISK ASSESSMENT:	Any impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity/business associate is able to demonstrate there is "a low probability that the [PHI] has been compromised based on a risk assessment" of the following four (4) factors, each of which should be deemed a low probability:[3] 1. Nature/extent of PHI involved, including types of identifiers and chance of re-identification; 2. The unauthorized person who used the PHI or to whom the disclosure was made; 3. Whether the PHI was actually acquired or viewed; and 4. The extent to which the risk to the PHI has been mitigated.

BREACH ACTION STEPS – If your risk assessment determines there is a potential breach of PHI, ***time is of the essence and thorough documentation is critical***. But do not rush or jump to conclusions. Key action steps include the following:	
CORRECTIVE ACTION AND INITIAL STEPS:	• If cause of potential breach is known or suspected, immediately implement remedy to reduce further acquisition, access, use or disclosure of PHI • Activate breach response plan and incident response team, which may include outside legal counsel, forensic team, law enforcement, and/or public relations team • Determine whether you have insurance coverage and whether vendor/3rd-party contracts require obligation to report incident • Complete investigation (i.e., identify type of incident, information compromised, complete the 4 factor risk assessment etc.) • Prepare and maintain an internal Data Breach Incident Report that describes in detail the discovery of the incident, steps in investigation, results from investigation, and how remedied • Develop communications strategy consistent with legal strategy and across all sectors
NOTICES AND REPORTING:	• Conduct legal assessment[4] as to whether notifications are required for affected individuals; if so, provide notice as required under HIPAA and/or state law; keep a log of notices/communications • After breach contained, full scope determined, and legal position developed, report incident to HHS's Office for Civil Rights ("OCR") if required; report incident to state if required • Create executive-level report of incident (high-level description, scope, impact, actions taken and recommendations)
FINAL STEPS:	• Conduct any necessary training for personnel and consider whether discipline is warranted • Harden your systems; ensure security is continually monitored to implement necessary updates • Maintain all evidence for at least six (6) years[5]

[1] 45 C.F.R. § 164.402.
[2] 45 C.F.R. § 164.402(1).
[3] 45 C.F.R. § 164.402(2).
[4] Note, this assessment should include legal counsel with experience in state and federal breach notification laws.
[5] 45 C.F.R. § 164.316. State law record retention requirements may differ.

Meg Pekarske
Hospice Practice Group Leader
Partner | Madison
608.234.6014
meg.pekarske@huschblackwell.com