HIPAA patch management policy

HIPAA variant: paste over the same-numbered sections of the general policy

1 Purpose and scope

1.1 This policy applies to every electronic information system of [Company name] that creates, receives, maintains or transmits electronic protected health information, and to every system that connects to one. [Company name] is a [covered entity / business associate].

1.2 The policy is part of the security measures required by 45 CFR 164.308(a)(1)(ii)(B), chosen on the basis of the risk analysis required by 164.308(a)(1)(ii)(A) dated [date].

4 Severity and patch windows

4.1 Risk level (critical, high, other) is assigned by the policy owner from the current risk analysis and recorded for each vulnerability.

4.2 Windows, from the date [Company name] identifies the need to patch, where a patch is available:

Risk level	Window now	Window if the proposed federal rule is finalized as written
Critical	14 calendar days (company standard)	15 calendar days
High	30 calendar days (company standard)	30 calendar days
All other	As set in the general policy	As set in this policy

4.3 Where no patch is available, the 15 and 30 days run from the date a patch becomes available, and Annex A applies meanwhile.

4.4 The company standard is stricter than or equal to every figure in the proposal, so adopting it now means no change when the rule is final.

9 Review and approval

9.1 This policy is reviewed and tested at least once every 12 months, and after any significant change to systems that hold ePHI.

9.2 Test means: [tabletop walk-through of one critical and one high case; evidence kept for each].

Annex A Exceptions (HIPAA)

A.1 An exception is valid only if (a) no patch is available, or (b) the only available patch would adversely affect the confidentiality, integrity or availability of ePHI.

A.2 Each exception records the compensating controls applied, the risk analysis entry, the approver and the date for the next check.