

The US proposes rules to make healthcare data more secure

The US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) is proposing new cybersecurity requirements for healthcare organizations aimed at protecting patients' private data in the event of cyberattacks, reports *Reuters*. The rules come after major cyberattacks like one that leaked the private information of more than 100 million UnitedHealth patients earlier this year.

The OCR's proposal includes requiring that healthcare organizations make multifactor authentication mandatory in most situations, that they segment their networks to reduce risks of intrusions spreading from one system to another, and that they encrypt patient data so that even if it's stolen, it can't be accessed. It would also direct regulated groups to undertake certain risk analysis practices, keep compliance documentation, and more.

The rule is part of the cybersecurity strategy that the Biden administration announced last year. Once finalized, it would update the Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which regulates doctors, nursing homes, health insurance companies, and more, and was last updated in 2013.

US deputy national security advisor Anne Neuberger put the cost of implementing the requirements at "an estimated \$9 billion in the first year, and \$6 billion in years two through five," writes *Reuters*. The proposal is due to be published in the Federal Register on January 6th, which will kick off the 60-day public comment period before the final rule is set.

<https://www.theverge.com/2024/12/28/24330878/the-us-proposes-rules-to-make-healthcare-data-more-secure>