Henry Ford Health Data Breach

Incident Name	Henry Ford Health Data Breach
Date of Public Report	July 18th, 2023
Date of Incident	March 3rd, 2023
Summary	Henry Ford Health is a Detroit based not-for-profit healthcare provider. On July 18, 2023, the company informed customers that it had been involved in a data breach on March 30, 2023 in which the personal information of 168,000 patients was exposed. The data included names, addresses, phone numbers, DOB, and lab results. The breach was the result of employees falling for a phishing campaign, after which the threat actor was able to gain unauthorized access to an employee email account which contained Private Health Information (PHI). Henry Ford Health has reported that the accounts have now been secured, and the company is now implementing additional security measures including employee security awareness training.
Key Social Engineering/OSINT Themes	• Recon - Employee and organizational information harvested. The hacker leveraged exposed employee information to conduct a social engineering attack. • Phishing - The attacker sent a convincing phishing email to certain employees. Once employees fell for the phishing campaign, the attacker gained access to their mailbox and exfiltrated PII and PHI data on customers.
Picnic's Recommended Remediations. For more, see the HASP Framework.	• User social engineering awareness training • Identify and block newly registered domains similar to your org's. This way if used in an attack (e.g., user clicking), the request to domain is blocked. • Monitor for expiring domains which could be leveraged for the above. • Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible. • Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is securely configured for all accounts. • Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party. • Regularly audit employee access to one of least privilege (including offboarding). • Regularly audit 3rd party access to one of least privilege. • Monitor and remove sensitive information disclosure.

Industry	Healthcare Services
Actor	Unknown
Motivations	Unknown
Related Hacks	MailChimp
Breach Notice/Company Notice	Breach Letter: https://www.henryford.com/-/media/files/hfh-patient-data-breach-substitute-notice-final-71423_pdf.pdf?rev=c4c7bc44f5b34de991947c5fe870d6d7&hash=1DCEC46FDA0242BF2BB609F790397C28
Other Sources	168,000 Patients Have PHI Exposed in Phishing Attack on Henry Ford Health : 168,000 Patients Have PHI Exposed in Phishing Attack on Henry Ford Health ; Henry Ford Health confirms data breach affecting 168,000 patients : Henry Ford Health confirms data breach affecting 168,000 patients