A Startup's Guide to HIPAA

Rock Health's guide to HIPAA
https://rockhealth.com/a-startups-guide-to-hipaa/

Architecting Your Healthcare Application for HIPAA Compliance

Medium post from AWS on privacy in digital health product development
https://medium.com/aws-activate-startup-blog/architecting-your-healthcare-application-for-hipaa-compliance-part-1-f3fbd11bd64d

---

HIPAA Compliance for Startups

Rock Health's startup support video
https://www.youtube.com/watch?v=rCPsN9d3eUc&index=19&list=PL706EB8B0816474FD

Ten Steps Towards Achieving HIPAA Compliance

A list with advice for achieving HIPAA compliance
https://itnow.net/10-simple-steps-towards-hipaa-compliance/

FDA Digital Health Innovation Plan

How does the FDA define digital health?
https://www.fda.gov/medical-devices/digital-health

EU General Data Protection Regulation (GDPR)

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

---

FDA Medical Device Cybersecurity Page

Includes premarket and post market management of medical devices
https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

---

Fact Sheet: the FDA's Role in Medical Device Cybersecurity

https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf

---

Hippocratic Oath for Connected Medical Devices

https://www.iamthecavalry.org/domains/medical/oath/

Manufacturer Disclosure Statement for Medical Device Security

Consists of the MDS form and instructions for completing it. Assists professionals responsible for security-risk assessment in the management of medical device security issues.
http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

---

AAMI TIR57

Provides medical device manufacturers with guidance on developing a cybersecurity risk management process for their products.
https://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729

Healthcare Industry Cybersecurity Task Force

Report on Improving Cybersecurity in the Healthcare Industry
https://healthsectorcouncil.org/health-care-industry-cybersecurity-task-force/

Health Industry Cybersecurity Practices (HICP)

Managing Threats and Protecting Patients – an industry-led effort in response to a mandate of the Cybersecurity Act of 2015 Section 405(d), to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the healthcare industry
https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/

Medical Device and Information Technology Joint Security Plan

Recommendations for manufacturing and managing the security of medical devices for clinical practice
https://healthsectorcouncil.org/hscc-releases-the-medical-device-and-health-it-joint-security-plan/

DHS CISA Resources for Small and Midsize Businesses

Resources to assist SMBs and startups with securing their organization. Includes roadmap for critical infrastructure requirements for small and midsize businesses
https://www.us-cert.gov/resources/smb

FCC Small Biz Cyber Planner

Helps businesses create and save a custom cyber security plan quickly to address specific business needs and concerns.
https://www.fcc.gov/cyberplanner

FTC Small Business Fact Sheet

Covers cybersecurity basics and best practices including the NIST cybersecurity framework for SMBs, and covers security threats (e.g. phishing, ransomware, email spoofing, and tech support scams, etc.)
https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

---

NIST Framework for Improving Critical Infrastructure Cybersecurity

Focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

---

DHS Entrepreneurs Tip Card

Provides simple cybersecurity tips and resources for entrepreneurs.
https://www.dhs.gov/sites/default/files/publications/Entrepreneurs%20Tip%20Card.pdf

---

HHS Quick Response Checklist for HIPAA Covered Entity or Business Associate

Provides HIPAA-related organizations brief guidance on responding to cyber incidents.
https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

---

HIPAA Security Rule and NIST Crosswalk

Identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule. This crosswalk maps each administrative, physical and technical safeguard standard and implementation specification1 in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework Subcategory.
https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

---

ISO/IEC 27000

Family of standards to help organizations keep information assets secure.
https://www.iso.org/isoiec-27001-information-security.html

Center for Information Security Top 20 Security Controls

https://www.cisecurity.org/controls/cis-controls-list/

OWASP Secure Medical Device Deployment Standard

A guide and checklist organizations can use as the basis for securely deploying network enabled medical devices
https://www.owasp.org/index.php/OWASP_Secure_Medical_Device_Deployment_Standard

---

OWASP Top Ten for Security - The Ten Most Critical Web Application Security Risks

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

---

UK Code of Practice for IOT

Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home
https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security

---

George Washington University workshop to develop a building code and research agenda for medical device software security

http://www.landwehr.org/2015-01-landwehr-gw-cspri.pdf

MITRE Secure coding course

http://opensecuritytraining.info/IntroSecureCoding.html

CWE/SANS Top 25 Most Dangerous Software Errors

https://www.sans.org/top25-software-errors

National Telecommunications and Information Administration Coordinated Disclosure Early Stage Template

https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

ISO29147

Provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services
https://www.iso.org/standard/72311.html

ISO30001

Guidelines for how to process and resolve potential vulnerability information in a product or online service
https://www.iso.org/standard/53231.html

I am the Calvary

List of manufacturers in cyber safety industries who have coordinated vulnerability disclosure programs
https://www.iamthecavalry.org/resources/disclosure-programs/

DHS CISA Vulnerability Disclosure Policy

https://www.us-cert.gov/vulnerability-disclosure-policy