PCI and HIPAA Compliance Guide
to Ensure Consistent Security & Confidentiality

THE HEALTHCARE INDUSTRY HAS BECOME A MAJOR TARGET FOR HACKERS AND SCAMMERS

In **2019**, the Healthcare industry had **THE SECOND MOST DATA BREACHES**, at 525 / second only to the business industry

89% of healthcare entities have had data breaches in the past two years

69% of Americans have had their PHI accessed in the last 10 years

41% of Americans have had their PHI breached in the last three years

A health record with basic insurance information is considered 10 – 20 times more valuable than a credit card with its information.

In **2020** alone, **32 MILLION PATIENT RECORDS HAVE BEEN BREACHED**

WHAT IS BEING DONE TO PROTECT YOUR VALUABLE DATA?

HIPAA REQUIREMENTS PROTECT PATIENTS' PRIVACY AND SECURITY.
HEALTHCARE OPERATIONS MUST COMPLY WITH THE FOLLOWING HIPAA GUIDELINES:

THE PRIVACY RULE

Protects PHI, keeping it hidden from outsiders, but also allowing it to be shared in house when necessary

THE ENFORCEMENT RULE

Gives specific guidelines for how to enact the rules of HIPAA and the ability to investigate potential issues within a system

THE SECURITY RULE

Establishes security standards that must be taken when health information is stored electronically

THE BREACH NOTIFICATION RULE

Requires HIPAA compliant entities to notify affected individuals

ADDITIONALLY, 41% OF HEALTHCARE ORGANIZATIONS ARE IMPLEMENTING FURTHER DIGITAL SECURITY PROGRAMS TO COMBAT HACKING ATTEMPTS

DATA BREACHES CAN ALSO GRANT HACKERS ACCESS TO CREDIT CARD INFORMATION

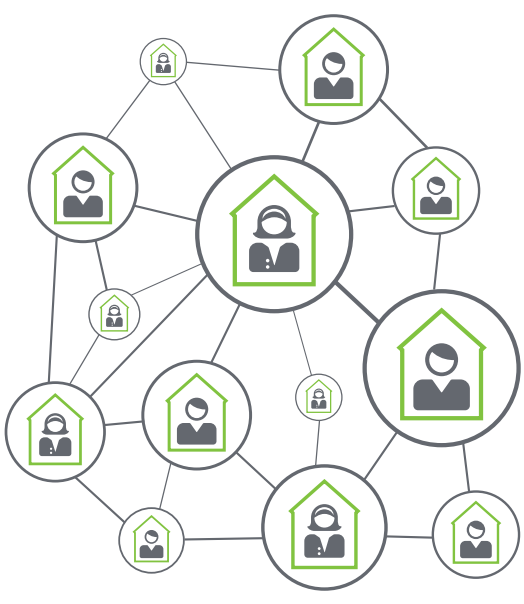
THIS IS WHERE PCI DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS) REQUIREMENTS COME INTO PLAY.

STEPS FOR MAINTAINING CREDIT CARD SECURITY BETWEEN CARDHOLDERS AND THE BUSINESS / ORGANIZATIONS THEY ARE PAYING

ARE YOU MEETING THE FOLLOWING REQUIREMENTS?:

- [ ] Install and maintain a firewall to protect cardholder data
- [ ] Create custom passwords for separate accounts
- [ ] Keep gathered data in a safe, encrypted location
- [ ] Encrypt transmission of cardholder data across open networks
- [ ] Use and regularly update antivirus software
- [ ] Develop and maintain secure systems and applications
- [ ] Restrict access to cardholder data by business need-to-know
- [ ] Identify and authenticate access to system components
- [ ] Restrict physical access to cardholder data
- [ ] Track and monitor all access to cardholder data
- [ ] Regularly test security systems and processes
- [ ] Maintain a policy that addresses information security

IS YOUR TEAM WORKING FROM HOME?
MAINTAINING PCI COMPLIANCE EVEN WHILE WORKING REMOTE



#1 OPTION ONE:
SECURE TERMINAL WITH A P2PE CREDIT CARD DEVICE

Determine whether your current credit card devices support taking payments from remote environments

#2 OPTION TWO:
SECURE TERMINAL WITH AN ENCRYPTED CREDIT CARD DEVICE

A non-P2PE credit card device has additional requirements to consider, as it has greater implications for the scope of PCI requirements

#3 OPTION THREE:
SECURE TERMINAL WITH DIRECT APPLICATION ENTRY

Direct Application Entry allows you to process a credit card without a device. This has greater implications for the scope of PCI requirements but removes the complexities of working with a credit card device

NO MATTER WHICH OPTION YOUR REMOTE WORKFORCE IS USING, IT IS IMPORTANT TO ENGAGE YOUR SECURITY TEAM AND QSA TO:

EXPLORE AND ASSESS YOUR OPTIONS

SEEK GUIDANCE AND RECOMMENDATIONS RELATED TO YOUR SECURITY AND COMPLIANCE POSTURE

GET APPROVAL BEFORE MAKING ANY SIGNIFICANT CHANGES TO YOUR REMOTE ENVIRONMENTS, SYSTEMS, POLICIES, AND PROCEDURES

WHILE HIPAA AND PCI ARE TWO SEPARATE SETS OF REQUIREMENTS FOR HEALTHCARE PROVIDERS, THEY BOTH ARE IN PLACE TO PROTECT PATIENT INFORMATION

HIPAA COMPLIANT — FOCUSES ON PATIENT MEDICAL RECORDS

PCI DSS COMPLIANT — IS CENTERED AROUND PAYMENT INFORMATION

HEALTHCARE DATA BREACHES HAVE ALMOST DOUBLED IN THE PAST FIVE YEARS

2015 — 270 breaches

2019 — 510 breaches

THE HEALTHCARE INDUSTRY IS INCREASINGLY TARGETED BY HACKERS,
MAKING THE SECURITY MEASURES OF HIPAA AND PCI MORE IMPORTANT THAN EVER

Source:

- bigcommerce.com/blog/pci-compliance/#what-is-the-pci-dss
- statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/
- ispartnersllc.com/blog/pci-dss-compliance-vs-hipaa-compliance/
- hhs.gov/hipaa/for-professionals/index.html
- hipaajournal.com/healthcare-data-breach-statistics/
- healthitsecurity.com/news/32m-patient-records-breached-in-first-half-of-2019-88-caused-by-hacking
- phoenixnap.com/blog/healthcare-cybersecurity-statistics
- impact-advisors.com/regulatory/pci-dss-compliance-in-the-connected-healthcare-environment/