
# HIPAA Security Risk Assessment

## Findings Report

**Brightmarsh Family Health**

Three Locations | Primary Care

## 1. Executive Summary

Barkrum conducted a HIPAA Security Risk Assessment of Brightmarsh Family Health across all three of its primary care locations. The assessment evaluated administrative, physical, and technical safeguards against the HIPAA Security Rule, with each location assessed on site rather than by sampling.

**Overall posture:** Moderate risk, with two high-severity findings requiring priority remediation. The practice demonstrates reasonable physical security and an established EHR environment, but lacks a documented risk analysis history and has unencrypted portable devices accessing electronic protected health information — the two gaps most consistently associated with enforcement action and breaches.

### FINDINGS AT A GLANCE


| Severity | Count | Meaning |
|---|---|---|
| **High** | 2 | Immediate risk to ePHI or clear regulatory exposure |
| **Moderate** | 4 | Meaningful gap requiring remediation on a defined timeline |
| **Low** | 2 | Minor gap; address as part of routine improvement |
| **Informational** | 1 | Observation or hardening opportunity, not a deficiency |

### FINDINGS SUMMARY

| ID | Finding | Severity |
|---|---|---|
| **HIPAA-01** | No documented risk analysis on record | High |
| **HIPAA-02** | Portable devices accessing ePHI without encryption | High |
| **HIPAA-03** | Business Associate Agreement gaps | Moderate |
| **HIPAA-04** | Shared front-desk workstation login | Moderate |
| **HIPAA-05** | Audit logs enabled but not reviewed | Moderate |
| **HIPAA-06** | Security awareness training lapsed | Moderate |
| **HIPAA-07** | Automatic logoff not configured | Low |
| **HIPAA-08** | Contingency plan never tested | Low |
| **HIPAA-09** | Server closet shares general storage | Informational |

### TOP THREE PRIORITIES

- Conduct and document this risk analysis, then establish it as an ongoing process. The absence of any prior documented analysis is itself the most commonly cited HIPAA failure.
- Encrypt all portable devices that store or access ePHI. Unencrypted laptops and mobile devices are the single most common source of reportable breaches.
- Close Business Associate Agreement gaps with the billing vendor and backup provider before any further ePHI is exchanged.

> **Regulatory basis:** *45 CFR 164.308(a)(1)(ii)(A) requires a covered entity to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. This report fulfils the format of that analysis.*

## 2. Scope and Methodology

This assessment covered all three Brightmarsh Family Health locations and the systems, devices, and workflows through which electronic protected health information is created, received, maintained, or transmitted.

### SCOPE

| In scope | Detail |
|---|---|
| **Locations** | All three primary care offices, each evaluated on site. |
| **Systems** | The electronic health record, practice management and billing systems, email, file storage, and backup. |
| **Devices** | Workstations, clinical laptops, and staff mobile devices with access to ePHI. |
| **People and process** | Workforce access, training, and the policies and procedures governing ePHI. |

### METHODOLOGY

The assessment followed the structure of the HIPAA Security Rule and the approach of the HHS Office for Civil Rights audit protocol. Work included the following:

- On site review at each location, rather than sampling one office and extrapolating.
- Interviews with practice leadership and workforce members on how ePHI is handled day to day.
- Inspection of technical configurations, including access control, encryption, logging, and backup.
- Review of existing policies, procedures, training records, and Business Associate Agreements.
- Mapping of each finding to the specific Security Rule provision it relates to.

> *Every finding in this report is tied to an exact regulatory citation, so the practice can verify each one against the rule itself and address it with confidence.*

## 3. Risk Rating Methodology

Each finding is assigned a severity that reflects both the likelihood that the gap is exploited or cited, and the impact if it is. The ratings are intended to help the practice sequence its work, addressing the most consequential gaps first.

| Severity | What it means | Expected response |
|---|---|---|
| **High** | Immediate risk to ePHI or clear regulatory exposure. | Address as a priority, ahead of lower rated items. |
| **Moderate** | A meaningful gap that should be closed on a defined timeline. | Plan and remediate within the current cycle. |
| **Low** | A minor gap, appropriate to address through routine improvement. | Fold into normal operations. |
| **Informational** | An observation or hardening opportunity, not a deficiency. | Consider as the program matures. |

> **A note on severity and enforcement:** *a high rating does not mean a violation has occurred. It means the gap is the kind most associated with breaches and enforcement, and therefore the most valuable to close first.*

## 4. Findings

| HIPAA-01 No documented risk analysis on record | HIGH |
|---|---|
| **Citation** | 45 CFR 164.308(a)(1)(ii)(A) |
| **Observation** | No prior HIPAA risk analysis could be located for any location. Staff indicated an assessment had not been performed since the EHR was adopted. |
| **Business Impact** | The risk analysis is the foundation of the entire Security Rule and the most frequently cited failure in OCR enforcement. Its absence exposes the practice to findings of willful neglect in the event of a breach or complaint. |
| **Recommendation** | Conduct and document a full risk analysis (this report), then establish it as a recurring process reviewed on change and periodically thereafter. |

| HIPAA-02 Portable devices accessing ePHI without encryption | HIGH |
|---|---|
| **Citation** | 45 CFR 164.312(a)(2)(iv); 164.312(e)(2)(ii) |
| **Observation** | Two clinical laptops and several staff mobile devices access ePHI without full-disk encryption enabled. Encryption is an addressable specification, but no documented alternative safeguard was in place. |
| **Business Impact** | Lost or stolen unencrypted devices are the single most common cause of reportable breaches. An unencrypted device breach is presumed reportable; an encrypted one generally is not. |
| **Recommendation** | Enable full-disk encryption on all devices that store or access ePHI, and document the decision and configuration as required for addressable specifications. |

| HIPAA-03 Business Associate Agreement gaps | MODERATE |
|---|---|
| Citation | 45 CFR 164.308(b)(1); 164.314(a) |
| Observation | No signed Business Associate Agreement was on file for the billing vendor or the offsite backup provider, both of which handle ePHI on the practice's behalf. |
| Business Impact | Sharing ePHI with a vendor absent a signed agreement is a direct violation and a recurring source of OCR settlements, independent of whether a breach occurs. |
| Recommendation | Execute Business Associate Agreements with the billing vendor and backup provider before any further ePHI is exchanged, and inventory all vendors that touch ePHI to confirm none are missed. |

| HIPAA-04 Shared front-desk workstation login | MODERATE |
|---|---|
| Citation | 45 CFR 164.312(a)(2)(i); 164.308(a)(4) |
| Observation | The front-desk workstation at two locations is used by multiple staff under a single shared login, so activity cannot be attributed to an individual. |
| Business Impact | Shared credentials defeat unique user identification and undermine audit logging, making it impossible to determine who accessed ePHI. This weakens both access control and accountability. |
| Recommendation | Provision unique credentials for each workforce member, and configure the workstation so that each user authenticates individually. |

| HIPAA-05 Audit logs enabled but not reviewed | MODERATE |
|---|---|
| Citation | 45 CFR 164.308(a)(1)(ii)(D); 164.312(b) |
| Observation | The EHR generates audit logs, but there is no procedure to review them, and no evidence that log review has occurred. |
| Business Impact | Enabling logs without reviewing them means suspicious access can go undetected. The Security Rule requires regular review of system activity, not merely its recording. |
| Recommendation | Establish a defined, periodic log review process with a named owner, and document each review so the practice can demonstrate the activity. |

| HIPAA-06 Security awareness training lapsed | MODERATE |
|---|---|
| Citation | 45 CFR 164.308(a)(5) |
| Observation | Security awareness training was delivered when the practice opened but has not been repeated. Several current staff have no record of completing it. |
| Business Impact | Untrained staff are the most common entry point for phishing and ransomware. Lapsed training is both a practical risk and a documentation gap in an audit. |
| Recommendation | Deliver security awareness training to all current workforce members, and set a recurring schedule with retained completion records. |

| HIPAA-07 Automatic logoff not configured | LOW |
|---|---|
| Citation | 45 CFR 164.312(a)(2)(iii) |
| Observation | Workstations do not automatically lock or log off after a period of inactivity, and several were observed unlocked and unattended in clinical areas. |
| Business Impact | An unattended, unlocked workstation in a patient area is an easy avenue to ePHI. Automatic logoff is a simple, addressable control that materially reduces this exposure. |
| Recommendation | Configure automatic logoff or screen lock after a short period of inactivity on all workstations that access ePHI. |

| HIPAA-08 Contingency plan never tested | LOW |
|---|---|
| Citation | 45 CFR 164.308(a)(7)(ii)(D) |
| Observation | A written backup exists and data is backed up, but the practice has never performed a test restore, and there is no documented contingency or emergency mode plan. |
| Business Impact | A backup that has never been restored may not work when it is needed. Ransomware and hardware failure both depend on a recovery capability the practice has not verified. |
| Recommendation | Perform and document a test restore from backup, and draft a brief contingency plan covering data recovery and emergency mode operation. |

| HIPAA-09 Server closet shares general storage | INFORMATIONAL |
|---|---|
| **Citation** | 45 CFR 164.310(a)(1); 164.310(d)(1) |
| **Observation** | The network and server equipment at the main location shares a closet used for general supply storage, accessed by staff without a business need for the equipment. |
| **Business Impact** | This is not a deficiency in itself, but co-locating infrastructure with general-access storage increases the chance of accidental or unauthorized physical contact with systems that hold ePHI. |
| **Recommendation** | Where practical, separate or lock the equipment so that physical access is limited to those with a need, and log access to the space. |

## 5. Risk Register

The register below records the risk determination for each finding: the likelihood that the threat is realized, the impact if it is, and the resulting risk level. Likelihood, impact, and risk level are rated on the scales described in Section 3, so the ratings here are consistent with the severities used throughout this report.

| Risk ID | Risk | Likelihood | Impact | Risk Level |
|---|---|---|---|---|
| **HIPAA-01** | Loss or theft of an unencrypted device holding ePHI, against the absence of a documented risk analysis | High | High | **High** |
| **HIPAA-02** | Loss or theft of an unencrypted portable device that stores or accesses ePHI | High | High | **High** |
| **HIPAA-03** | ePHI shared with vendors that have no signed Business Associate Agreement in place | Moderate | Moderate | **Moderate** |
| **HIPAA-04** | ePHI access under a shared login that cannot be attributed to an individual | Moderate | Moderate | **Moderate** |
| **HIPAA-05** | Unauthorized ePHI access going undetected because audit logs are not reviewed | Moderate | Moderate | **Moderate** |
| **HIPAA-06** | Workforce falling to phishing or mishandling ePHI due to lapsed training | Moderate | Moderate | **Moderate** |
| **HIPAA-07** | Unattended, unlocked workstation exposing ePHI in a patient area | Low | Moderate | **Low** |
| **HIPAA-08** | Inability to recover ePHI because backups have never been test restored | Low | Moderate | **Low** |
| **HIPAA-09** | Physical contact with server and network equipment stored in a general access closet | Low | Low | **Low** |

**How to read this register:** *each risk level is derived from its likelihood and impact using the standard matrix in Section 3. The remediation roadmap that follows sequences these risks so the highest are addressed first.*

## 6. Remediation Roadmap

The following sequence groups the findings into a practical order of work, priority first. Suggested owners are indicative; the practice should assign them to the appropriate staff or vendor.

| Priority | Findings | Suggested owner |
|---|---|---|
| **Immediate** | HIPAA-01 (risk analysis), HIPAA-02 (encryption), HIPAA-03 (BAAs) | Practice leadership with IT support |
| **Near term** | HIPAA-04 (unique logins), HIPAA-05 (log review), HIPAA-06 (training) | Office manager with IT support |
| **Routine** | HIPAA-07 (automatic logoff), HIPAA-08 (backup test) | IT support |
| **As program matures** | HIPAA-09 (equipment separation) | Practice leadership |

> *Closing the three immediate items resolves both high-severity findings and the most commonly penalized gap, materially improving the practice's posture and its position in the event of a breach or audit.*

## 7. Safeguard Posture Summary

This summarizes the practice's posture across the three safeguard categories of the HIPAA Security Rule, as a high-level view of where attention is most needed.

| Safeguard category | Posture | Summary |
|---|---|---|
| **Administrative (164.308)** | Needs work | The core gaps are here: no documented risk analysis, lapsed training, unreviewed logs, and BAA gaps. |
| **Physical (164.310)** | Reasonable | Physical security is generally sound; the one item is shared use of the equipment closet. |
| **Technical (164.312)** | Mixed | An established EHR and audit logging are in place, offset by unencrypted devices, shared logins, and no automatic logoff. |

**The headline:** *the practice's technical foundation is workable, and its physical security is sound. The concentration of risk is administrative, and the single most valuable action is to establish the documented risk analysis and management process that the rest of the program depends on.*

## 8. About This Assessment

This assessment was performed by **Barkrum**, led by a Certified Information Systems Auditor (CISA, from ISACA, the Information Systems Audit and Control Association). Every location is assessed on site, findings are tied to exact regulatory citations, and engagements are delivered on a fixed scope and fixed fee.

The independent audit authority behind this report is what distinguishes it from a self assessment. A self assessment surfaces only the risks an organization already knows it has; an assessment performed and signed by an independent, credentialed party is what withstands scrutiny when a regulator examines it.

> **This report is illustrative and fictional.** *Brightmarsh Family Health does not exist, and no real patient, client, or organizational data appears anywhere in this document. It is provided as a sample of Barkrum's HIPAA Security Risk Assessment deliverable.*