



## **HIPAA Communications Playbook for Healthcare Practices**

How to standardize phone, voicemail, texting, fax, and after-hours workflows across your team so they run consistently every day.

# Table of Contents

---

## 03

How to Use This Playbook

---

## 04

What to Verify for HIPAA  
in Communications

---

## 05

Where Communications  
Workflows Break Down

---

## 07

The Controls That Keep  
Workflows Consistent

---

## 09

Which Vendors Need a BAA  
and What to Confirm

---

## 11

Patient Messaging and  
“Reasonable Safeguards”

---

## 13

Download the Communications  
Governance Checklist

---

## 14

What to Do Next

---

# How to Use This Playbook

---

Clinic communications are where HIPAA risk shows up day to day. Voicemail, texting, fax, call routing, and after-hours coverage are high-volume workflows. When they're handled differently by location, shift, or staff member, gaps show up fast.

This playbook is for the clinic admin or ops lead who needs those workflows to run consistently every day. It focuses on the controls that make that possible: role-based access that's removed promptly when staff changes, audit history you can pull when needed, patient communication

preferences that are recorded and visible to the team, and vendor agreements that match the tools that store or process your communications data.

Use the playbook in two passes. First, confirm you can answer those basics without guessing. Then standardize one workflow at a time, starting with the area where your team is most likely to improvise. Keep access, templates, and vendor coverage consistent. That makes the rest easier to manage.

## Want a working version of this framework?

Download the [Communications Governance Checklist](#) to review access, messaging, routing, after-hours rules, and vendor controls across your practice.



# What to Verify for HIPAA in Communications



The HIPAA Security Rule covers electronic protected health information (ePHI) any time it is created, received, stored, or transmitted. In communications workflows, exposure is often operational rather than just technical: one location handles voicemails one way, another forwards messages differently, and after-hours rules vary by team.

## Where ePHI shows up in communications workflows

In most clinics, ePHI shows up in two places: the content and the trail. The content is voicemail, transcriptions, message threads, fax images, and recordings. The trail is call history, routing history, and activity logs that show who accessed or changed something and when.



If you cannot answer “**who accessed what, and when,**” you do not have a defensible communications workflow.

## What you should be able to verify and defend

You do not need to quote regulations in a meeting. You need to know whether your system supports three basics:

- ✓ **Access Control:**  
You can limit who can access ePHI and manage user access across locations and shared teams.
- ✓ **Audit Controls:**  
You can record and review activity in voicemail, messaging, fax, and administrative access.
- ✓ **Transmission Security:**  
You can protect ePHI while it is in motion.

If a vendor cannot explain how these apply to your real workflows, you will end up relying on tribal knowledge and workarounds. In multi-location clinics, workarounds spread fast.

# Where Communication Workflows Break Down



In clinics, communication risk usually comes from workflow drift. The same patient scenario is handled differently across sites, shifts, or staff members, and over time, that makes it harder to control and document what's actually happening.

## Voicemail and Transcription

Voicemail is one of the most common places ePHI shows up, and one of the easiest places for access to drift. The question is who can access it, from where, and whether that access is reviewed. Shared mailbox credentials, unclear ownership, and old staff accounts are common warning signs.

A simple test is this: can you explain who has access to voicemail and transcriptions across locations, and can you review that access without relying on memory? If the answer is "it depends on the site," you have a governance problem.

## Patient Messaging and Texting

Staff want speed, patients want responsiveness, and "just send a quick message" can turn into sensitive details traveling through the wrong channel. You see it when different sites use different templates, different escalation rules, and different habits for what goes into a message.

**Policy needs to be explicit:** what belongs in a routine text, what does not, and how you handle patient requests for confidential communications. Standardize routine message content, when staff should switch channels, and how patient communications are managed and retained.

## Fax Intake and Outbound Routing

Faxing is a common workflow for referrals, labs, and payers. The main risks are misdirection, uncontrolled access at receipt, and weak tracking. In multi-location clinics, routing adds another layer: who is allowed to send and receive, where faxes land, and who confirms the right destination.

The practical takeaway is to standardize verification steps and access controls.

## Call Routing, Shared Lines, and Handoffs

Routing and handoffs are where multi-location complexity shows up most clearly. Calls move between front desk teams, clinical staff, billing, and on-call coverage. Common failure points are different routing rules by location, different definitions of urgent, and unclear ownership of escalations.

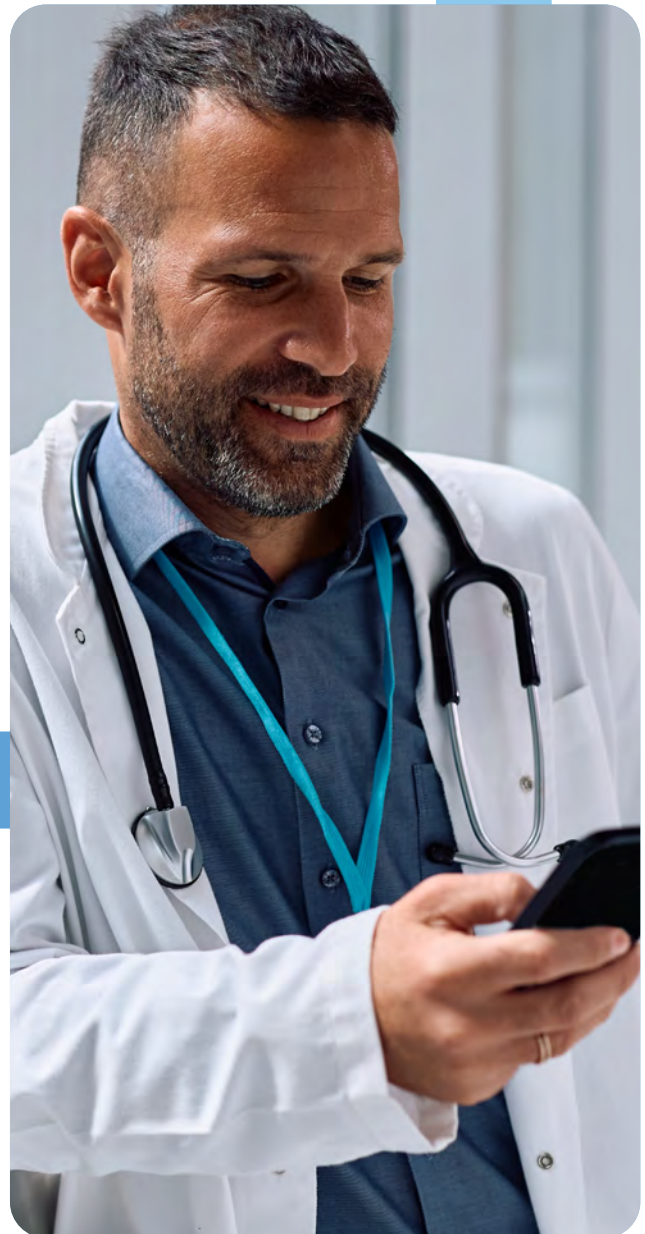
If you cannot trace what happened to an inbound patient call, you cannot show that the workflow is controlled.

**In multi-location clinics, exposure often comes from drift:** the same patient scenario handled three different ways across three sites.

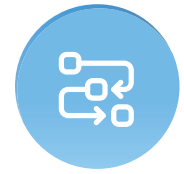
## After-hours Escalation and Answering Services

After-hours is a predictable risk zone because the workflow changes when the clinic is closed. Calls may be forwarded to an answering service, an on-call provider, or a rotating team. Drift shows inconsistent escalation rules, ad hoc forwarding, and unclear boundaries between what can be handled by phone and what should be handled through a secure workflow.

Vendors become part of the workflow quickly here. If a third party handles after-hours messages and has access to ePHI, you need clear responsibilities and documentation, not just **"they are our answering service."**



# The Controls That Keep Workflows Consistent



- ✓ You can also use the [Communications Governance Checklist](#) to review those same controls in a working format across your practice.

The risk areas above—voicemail, messaging, fax, routing, after-hours—share the same underlying control requirements. The practical question is whether you can control access, review what happened later, follow patient communication preferences, and document which vendors are involved. Most can't answer all four without guessing.

If you are evaluating communications tools, start with four questions: who has access, what can you review later, how are patient communication preferences handled, and which vendors are inside the workflow?

[NIST SP 800-66 Rev. 2](#) is a government backed implementation guide for the Security Rule, written for regulated entities of all sizes. It's a useful reference if you need to document risk-based decisions for communications workflows.

## Access control

Access control means you can limit who can access ePHI and manage that access consistently across locations and roles—without depending on shared logins or informal handoffs to get work done.

The fastest way to pressure-test access control is to ask where ePHI lives and who can see it. Who can access voicemail history? Who can access fax history? Who can access patient message threads? Who can change call routing or after-hours rules? If the answer depends on location, you do not have a single operating model.

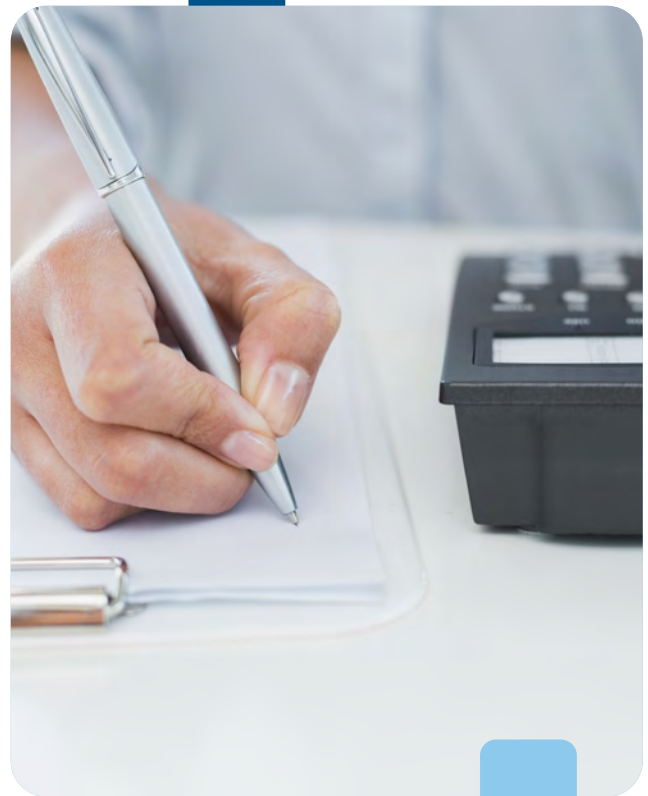
## Audit controls

Audit controls mean you can record and examine activity in systems that contain or use ePHI, so you can answer "who did what, when" without guessing.

Vendors often oversimplify this. "We log activity" is not enough. You need to know what is logged, who can review it, how long it is retained, and whether you can pull a usable record quickly when you need it.

## Transmission Security

Transmission security means ePHI is protected while it is moving between devices and systems. If your staff use mobile devices, home networks, or work across locations, this applies to every shift.



## Admin Integrity and Authentication

In a multi-location clinic, this means predictable admin workflows, role-based permissions, and access that can be removed immediately when someone leaves. If someone can change routing rules or voicemail scripts without a trace, you do not have a controlled workflow.

### What To Verify, In Plain Terms

- ✓ **Auditability:**  
We can see who accessed or changed something and quickly pull that history.
- ✓ **In-Transit Protection:**  
We can explain how ePHI is protected when it moves between devices and systems.
- ✓ **Admin Changes:**  
We can trace routing, after-hours, and permission changes.

If your controls depend on **“how this location does it,”** they will not hold up under pressure.

# Which Vendors Need a BAA and What to Confirm



**In a multi-location clinic, communications vendors often touch more ePHI than teams expect:** voicemail storage, call logs, message threads, faxes, transcriptions, recordings, and after-hours coverage. If a vendor creates, receives, stores, or transmits that data on your behalf, treat them as part of your HIPAA program.

A BAA tells you which vendors are formally accountable, what they are responsible for, and what the process is if something goes wrong.

## What Makes a Communications Vendor a Business Associate

A vendor is generally a business associate when they create, receive, store, or transmit ePHI on your behalf and do more than pass data through without storing it. In practice, most hosted communications platforms store voicemail, logs, messages, recordings, or fax images, which usually puts them inside that definition.

## Default Assumption for Multi-Location Clinics

*If the vendor stores your communications data, assume they are a business associate and require a BAA. If a vendor claims they are only a conduit, ask them to explain exactly what data they store, for how long, and who can access it.*

## What to Confirm in a BAA for Communications Workflows

This ebook isn't legal advice. It's a sanity check: make sure you have a BAA that actually covers what you use, and don't treat vendor marketing copy as a substitute for a contract.

Start by confirming that the BAA explicitly covers the data generated by your communications workflows: voicemail, transcriptions, messaging content, fax images, call records, recordings, and administrative logs. If a vendor provides only a generic BAA that does not map to the specific services you use, you may be accepting gaps you cannot defend later.

## What To Document So Your Vendor Choices Are Defensible

Keep three things in one place and up to date as you add locations, change staff, and swap tools.

- ✓ **1. Vendor Inventory**  
**List every vendor that touches communications ePHI:** phone/VoIP, messaging, fax, transcription, call recording, answering services, and any storage or forwarding services. Update it when you add a location or change workflows.
- ✓ **2. BAA File**  
**Keep a signed BAA for each vendor in one place,** and track renewal dates and subcontractors. If a vendor will not sign a BAA, treat that as a decision point, not a footnote.
- ✓ **3. Risk Notes**  
**If you accept any risk-based exception,** record why it was reasonable for your environment and what mitigation you put in place.

Once your vendor inventory is current and BAAs are on file, confirm the specifics.

If you do not know where voicemail, transcriptions, messages, and recordings are stored, **you do not know which vendors are inside your HIPAA program.**

## BAA Checklist for Communications Vendors

Keep three things in one place and up to date as you add locations, change staff, and swap tools.

### Access and Auditability

Confirm the BAA supports access control and auditability expectations, and that you can obtain the information you'd need to investigate an incident. If you can't get usable audit history without delay or negotiation, you may not be able to answer basic questions during an audit or investigation.

### Subcontractors

Confirm whether subcontractors are involved for storage, transcription, messaging, or analytics, and that your vendor follows the same safeguards and restrictions down to them. If the vendor can't describe subcontractors, you can't realistically manage risk across locations.

### Incident reporting

Confirm how incidents are identified, escalated, and reported to your clinic, and what cooperation looks like during investigation. Multi-location workflows make it easy to miss issues, so notification expectations need to be explicit.

### Data Retention and Termination

Confirm what happens to message history, fax archives, call logs, recordings, and transcriptions at termination, and how data is returned or destroyed. This also affects migrations and legal holds.

### No Secondary Use of PHI

If the vendor uses AI or automated transcription, confirm that the BAA prohibits using PHI to train models or for any secondary purpose unless explicitly authorized. Don't rely on a marketing statement for this.

# Patient Messaging and “Reasonable Safeguards”



Texting is often where staff start making exceptions. Patients miss reminders, messages arrive late, someone gets a text meant for another day, and staff improvises to keep the schedule moving.

HIPAA does not ban electronic communication with patients. It expects **reasonable safeguards** and clear handling when a patient requests a specific communication method.

## What Belongs in a Routine Message

A messaging policy only works if staff can follow it on a busy day. Define what belongs in a routine message and what does not.

Routine messages should be operational and neutral. Think scheduling, confirmations, simple logistics, and callback requests. Avoid diagnoses, test results, detailed clinical discussions, or anything that would surprise a patient if someone else saw it on their lock screen.



## What To Do When a Patient Requests Texting or Unencrypted Email

Patients can request that you contact them in a specific way or at a specific number, and you are required to accommodate reasonable requests. That does not mean everything should be texted. You need a consistent way to handle patient requests and document them.

Treat this as an operations workflow, not a judgment call. Decide who can approve the request, where it is documented, and what the default content rules are for that channel.

## Simple Rule For Busy Days

If the content would create harm or embarrassment if read by the wrong person, **it does not belong in a routine text.**

Messaging works when the rules are **simple, consistent, and easy to audit.**

## Minimum Necessary and Templates

Build a small set of templates that cover your most common scenarios: appointment reminders, missed calls, rescheduling, billing callbacks, and document requests. Keep them short. Keep them neutral. Make it easy for staff to use templates instead of typing from scratch.

Templates help keep message content consistent across sites. If one location includes extra clinical context and another keeps messages neutral, you have an inconsistency that is hard to defend.

## Where Texting Creates Risk in Multi-Location Clinics

Most texting risks come from:

- ✓ **1. Mixed Tools**  
If one site uses one messaging tool and another uses a different one, policies drift, and it becomes difficult to audit.
- ✓ **2. After-Hours Texting**  
When after-hours routing relies on texting, the boundary between "triage" and "clinical guidance" can blur.

## What To Verify in Your Messaging Workflow

- 1. Staff do not need to use personal devices or personal numbers.*
- 2. Message access is role-based and can be removed immediately when someone leaves the role.*
- 3. Message history and activity can be reviewed when needed.*
- 4. Templates exist for common scenarios, and staff actually use them.*
- 5. Patient requests for a specific communication method are documented and followed.*

## How to Keep This Practical

Do not try to solve every edge case in policy. Standardize the default: neutral messages, templates, and clear ownership of message queues. Define a single path for exceptions—patient requests and sensitive situations—and handle them consistently every time.

The [Communications Governance Checklist](#) can help you review those messaging rules, exception paths, and ownership controls across your practice.

# Download the Communications Governance Checklist: Review Access, Messaging, Routing, & Vendor Controls



---

## **[Download the Communications Governance Checklist here.](#)**

Use this checklist to review the controls that keep phone, voicemail, texting, fax, and after-hours workflows consistent across your practice.

### **Access & Permissions**

Role-based access, offboarding, shared inbox visibility

### **Messaging Preferences**

Patient preferences, exception handling, routine message rules

### **Workflow Ownership**

Routing, voicemail, fax, queue ownership, after-hours responsibilities

### **Vendor Documentation**

BAAs, vendor inventory, subcontractors, retention records

### **Templates & Training**

Message templates, voicemail scripts, staff training, escalation rules





## RingRx Buyer Check

If you are evaluating RingRx or any healthcare communications vendor, ask these questions and expect clear answers:

- *Does the vendor sign a Business Associate Agreement?*
- *Which communications data may contain PHI, including voicemail, fax, message history, call logs, recordings, and transcriptions?*
- *How is access controlled across locations, roles, and shared teams?*
- *What activity can be reviewed later, and how quickly can audit history be pulled?*
- *How are patient communication preferences recorded and followed in day-to-day workflows?*
- *What happens to communications data at termination, migration, or account changes?*



## What to Do Next

Start with the highest-volume workflow where staff are most likely to improvise. For that workflow, confirm who has access, what you can review later, how patient communication preferences are recorded, and which vendors and BAAs are in scope.



Then use the [Communications Governance Checklist](#) to review the rest. You can download it as a standalone resource and use it for quarterly reviews, staffing changes, vendor onboarding, or workflow updates.

If you want to know how RingRx can support these workflows in your environment, [contact us today](#).



## Book a Demo today!

Discover how RingRx can enhance your practice's communication and streamline operations. [Book a demo](#) today or call (888) 980-6860 to see how we can tailor our solutions to fit your organization's needs.





888-980-6860



info@ringrx.com



1900 State St, Ste L, Santa Barbara, CA 93101

[www.RingRx.com](http://www.RingRx.com)