



WHITE PAPER · FOR MEDICAL AND DENTAL PRACTICE OWNERS,
ADMINISTRATORS, PRIVACY OFFICERS, AND IT DECISION MAKERS

Protecting patient information in business phone systems

A HIPAA procurement guide for medical and dental
practices with a separate veterinary privacy discussion

Compliance rests on the data workflow, contracts, and operating
safeguards. Hosting location or an encryption feature cannot
establish it alone.

PUBLISHED BY
Greg Steinig, SPARK VoIP

DATE
October 2026

RESEARCH REVIEWED THROUGH
October 4, 2026

Executive summary

Medical and dental practices should evaluate a phone system by the information it creates, stores, sends, and exposes to people. A voicemail, recording, transcript, email copy, or appointment message can produce a new data location. Each location needs a defined purpose, access policy, retention approach, and accountable provider.

The Health Insurance Portability and Accountability Act (HIPAA) applies to covered entities and business associates. The US Department of Health and Human Services (HHS) identifies covered health providers by specified electronic transactions. [1] Animal-only treatment records do not become human protected health information (PHI) from the patient label; that distinction is an inference from the definitions, not an HHS veterinary determination. Assess unusual human-data relationships separately. [6]

HHS distinguishes transient transmission from maintaining electronic PHI (ePHI). Persistent cloud storage can create business-associate duties even without the decryption key. [2, 3] Map business associate agreements (BAAs) through the contracting chain; separately purchased services need their own role and agreement review. A phone provider's BAA does not cover every outside service. [7]

Key findings

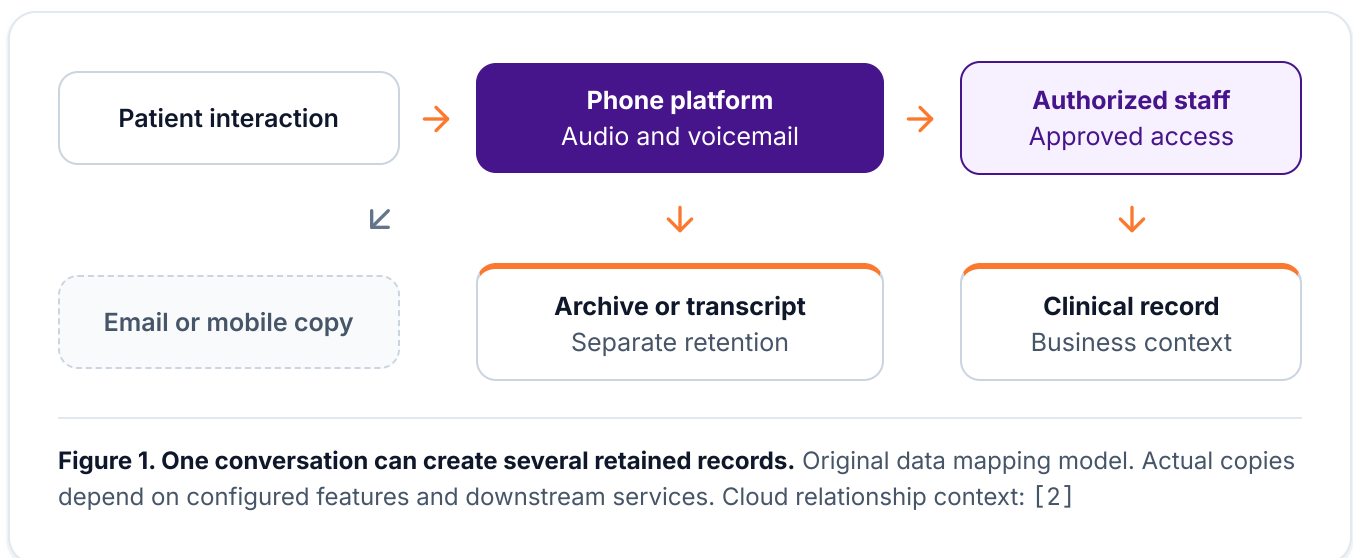
- 01 Determine covered-entity and business-associate status before requesting a label. [1]
- 02 Stored voicemail and recordings can change the provider relationship. [2, 3]
- 03 A BAA does not replace the practice's risk analysis or operating safeguards. [4]
- 04 Email copies and transcripts expand the data workflow.
- 05 Where a system is hosted is one input; the workflow, contracts and safeguards decide compliance.

The purchasing result should be a documented data map, appropriate contracts, provider operating evidence, and tested safeguards for each approved workflow. This guide covers ordinary US medical and dental communications, with a separate veterinary scope discussion. It does not certify a deployment.

Map information beyond the live call

A live conversation and a saved copy have different lifecycles. The conversation can end, but an audio file may remain on the platform, in an archive, in email, and on a user's phone. A transcript can persist after the recording is deleted. Procurement should identify all these copies before the practice turns on convenient sharing features.

Name the information needed for each task. A callback may need a number and limited message rather than a full clinical narrative. Clinical content may need an entry in the health record system. Decide which records must be preserved before setting routine deletion; a phone retention setting is not a complete medical-record schedule.



For every arrow in the data map, ask who receives the information and what contract and safeguard apply. A personal mailbox or unmanaged smartphone can undermine controls that are strong on the server. Disable a workflow when its receiving destination cannot meet the practice's requirements.

Match contracts to provider behavior

HHS's audio-only guidance explains that a telecommunications service acting only as a conduit does not require a BAA for that transmission role. Persistent access or storage changes the analysis. The answer should follow what the service does, rather than whether it is marketed as a

telephone company. [3]

Table 1. Provider roles and questions for contracting

Service behavior	Relationship question	Evidence to request
Transient transmission only	Does the conduit analysis apply?	Written scope and actual access behavior
Maintained voicemail or recordings	Does the provider maintain ePHI?	BAA scope, retention, and safeguards
Cloud archive	Which entity maintains each stored copy?	Direct or downstream BAA responsibility, retrieval, retention, and disposition
Transcription or analytics	Who receives audio and resulting text?	Approved processing purpose and downstream contracts
Email or practice software	Which destination receives the information?	Account controls, contract, and access policy

Contracting framework derived from HHS role distinctions. It is not a determination for a specific provider. [2, 3]

Before approving a regulated workflow, obtain the service-specific BAA and identify its legal parties, permitted uses, reporting terms, subcontractor obligations, access, and termination provisions. [8] Match the agreement to every approved processing activity, including voicemail, storage, and any transcription. A promise to sign later is not an executed agreement.

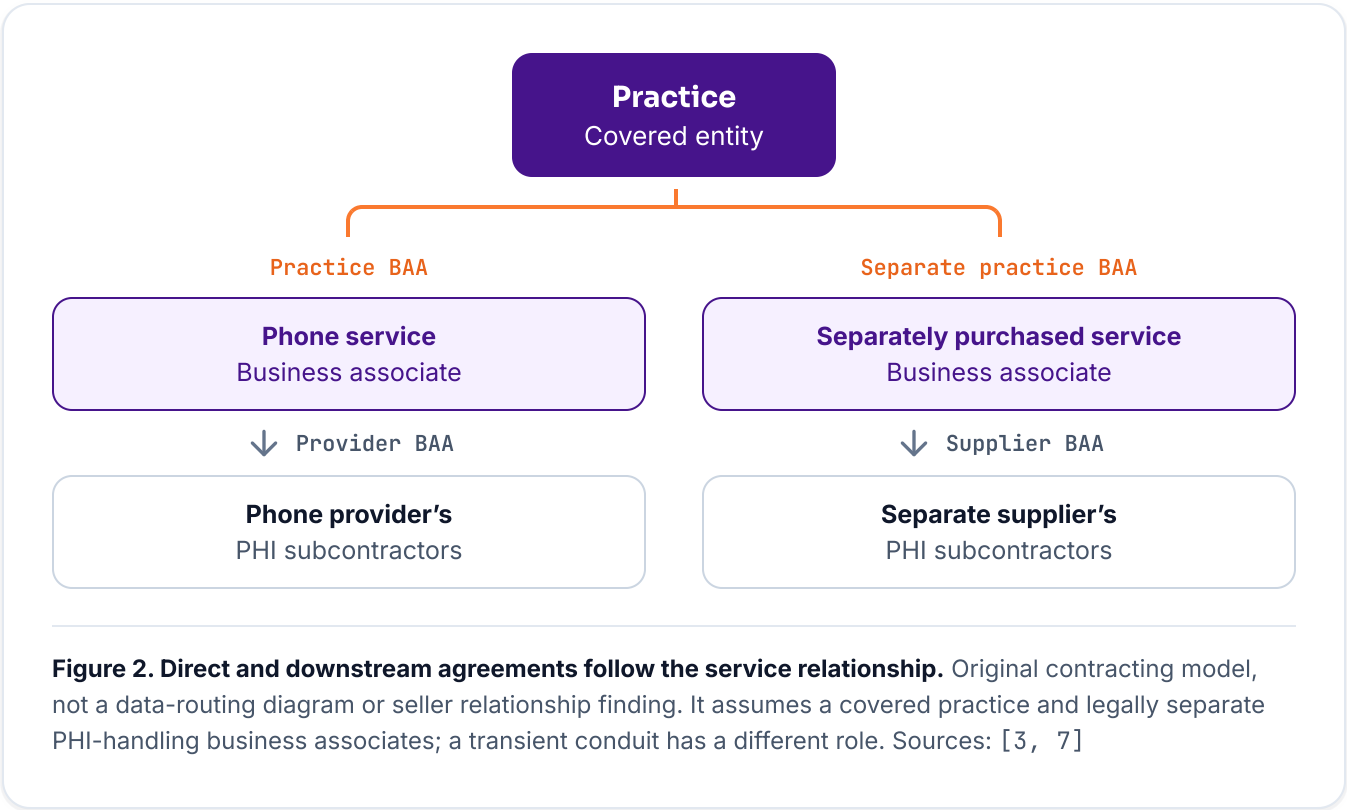
A transient conduit and a maintained-data service require different role analysis. A service that stores encrypted ePHI cannot claim conduit status solely from lacking its decryption key. [2, 3] Verify behavior, not a product label or an unsupported statement about liability for every call.

SPARK VOIP BUSINESS ASSOCIATE AGREEMENT

SPARK VoIP signs a business associate agreement with medical and dental practices for its hosted service. Request it with your proposal and match its scope to the workflows you approve.

Separate the contract chain from the data flow

For an ordinary covered-entity relationship, the practice obtains a BAA with its business associate. That associate obtains the required agreement with its PHI-handling subcontractor. The practice need not obtain a separate BAA directly from every downstream subcontractor. [7] Confirm who is directly engaged and who acts downstream; the diagram assumes each shown supplier is a business associate.

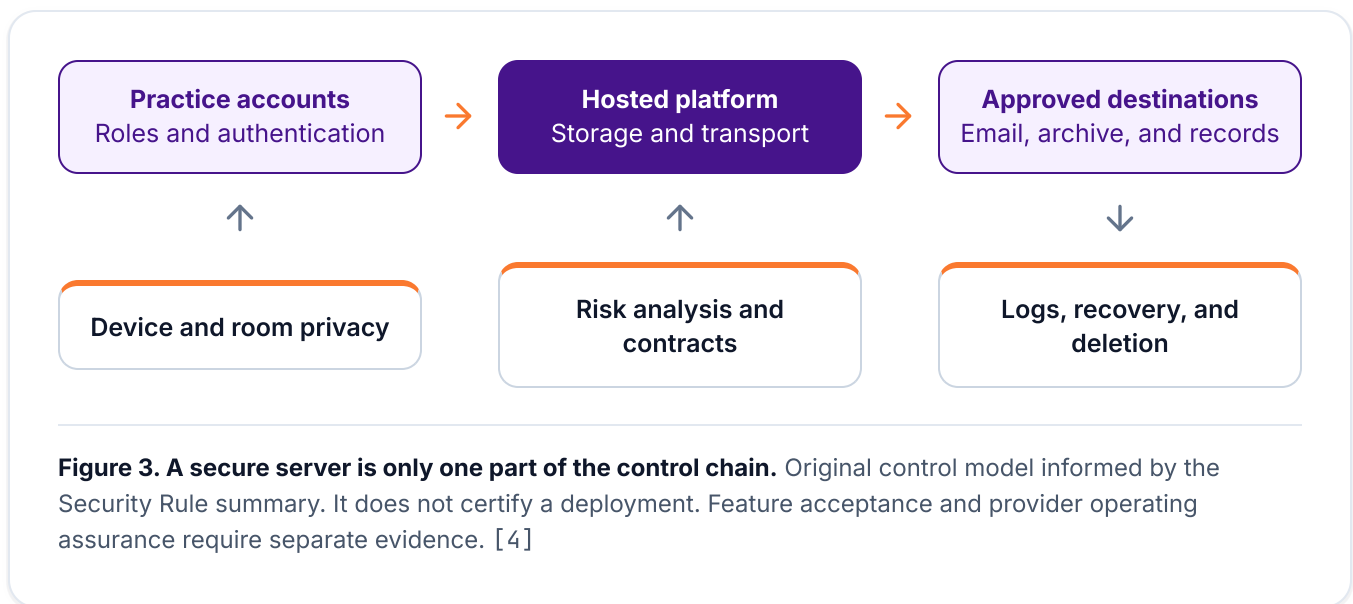


A separately purchased email, transcription, or records service sits on its own contracting path. A phone-service agreement does not automatically cover it. Reconcile the legal-party inventory with the data map, including support access and outsourced storage. Record permitted processing and confirm the provider’s downstream obligations; do not infer coverage from a supplier logo.

Collect executed service-specific agreements, the approved downstream service inventory, and evidence of applicable subcontractor commitments. Ask who handles incidents, access requests, record retrieval, and termination. Ask SPARK VoIP to identify the legal parties and demonstrate how the proposed scope covers your approved workflows.

Verify safeguards across the whole workflow

HHS describes administrative, physical, and technical safeguards, including risk analysis, access and audit controls, and contingency planning. Addressable specifications require a reasoned, documented assessment; they are not optional by label. [4] The current eCFR text retains this framework. The HHS Security Rule proposal page states that the current rule remains in effect during rulemaking; proposed changes are not treated as enacted duties here. [7, 11]



Recommended design requirements include supported transport and storage encryption, unique accounts, role-based access, multifactor authentication, monitored administration, and tested recovery. Demonstrate the selected configuration across the approved destinations. Record unavailable controls and the risk decision; do not describe a requested safeguard as a tested product capability.

Ask the provider which events its logs actually capture. A log of administrative configuration changes is not automatically a log of every recording playback or download. The practice should know whether it can identify the person, action, record, and time for the access events its policy requires.

For each call or file path, identify protocols, encryption endpoints, key custody, and any carrier or application handoff. Verify public-network segments separately rather than extending a hosting-provider claim across the entire conversation. No end-to-end encrypted path was demonstrated for this paper. An encryption checkbox is insufficient acceptance evidence.

Verify provider operating controls

A feature test shows behavior at a particular time. Provider assurance concerns how access, updates, incidents, and recovery are managed over time. Section 164.308 addresses risk analysis, activity review, security incidents, and contingency planning. [7] Table 2 is a recommended evidence request, not a list of universally prescribed audit documents.

Table 2. Provider operating evidence for the proposed service

Control area	Primary evidence to request	What the practice should check
Risk and service scope	Dated risk assessment scope, responsibility register, and unresolved-risk treatment.	Phone application, storage, support, and downstream services are covered; practice tasks are assigned.
Patching and vulnerability handling	Supported-version inventory, update process, and redacted remediation records.	Who acts, how urgent fixes are handled, which assets are omitted, and how completion is recorded.
Privileged support access	Roles, approval and revocation process, authentication, and sampled administrative activity records.	Support can reach only the approved scope; access is attributable, reviewed, and removed when no longer needed.
Incident and outage response	Response procedure, escalation contacts, reporting terms, and exercise or incident follow-up.	Provider and practice responsibilities align; contacts, decisions, and notification routes are usable.
Recovery and independent assurance	Witnessed restore and outage retrieval results; relevant assurance report scope, period, and exceptions if available.	Tested recovery covers the selected service. An audit of a datacenter alone is not evidence for every application or workflow.

Original procurement matrix informed by [7]. Document the evidence date, scope, exceptions, reviewer, and unresolved items. An assurance report is one input, not a HIPAA certificate. Request provider operating evidence for the proposed scope.

Compare company-owned and third-party hosting against the same evidence. Owned hosting may give closer control yet concentrate failure and staffing dependencies; third-party hosting may supply broader operating resources yet add contractual and dependency work. These are tradeoffs to investigate, not measured advantages of either model. Assign the provider and practice controls in writing.

Plan preservation and disposition for each copy

HHS states that the Privacy Rule does not set medical-record retention periods; state law often governs them. [9] Section 164.316(b) separately requires six years for specified Security Rule documentation, measured from creation or last effective date, whichever is later. That is not a universal six-year rule for every recording. [10] Use a records specialist or counsel to set the applicable schedule and preservation duties.

Table 3. Record retention and disposition planning matrix

Record or copy	Preservation decision and owner	Routine disposition and proof
Voicemail or recording	Records lead decides clinical-record status, applicable schedule, and hold triggers.	Provider documents active-storage deletion and surviving copies; retain tested results.
Transcript or summary	Clinical and records leads approve the entry, corrections, retention, and preservation.	Trace audio and text separately; deletion of one does not prove removal of the other.
Email attachment or export	Records and technology leads identify mailboxes, downloads, recipients, schedule, and holds.	Test each controlled destination; log unresolved or unmanaged copies and required follow-up.
Clinical record entry	Clinical records owner applies the governing health-record schedule and preservation duties.	Use the approved clinical-record process, not the phone platform's deletion setting.
Backup or archive	Provider and records lead reconcile backup cycle, hold handling, restoration, and retained-copy access.	Record expiration dates and exceptions; test whether restore reintroduces deleted records and how disposition is reapplied.

Original recommended matrix, not an approved record schedule. Complete record-specific durations, hold decisions, accountable names, and evidence before routine disposition; no deployment result is asserted.

Do not confuse routine deletion with termination duties. Section 164.504(e)(2)(ii)(J) requires contractual return or destruction of retained PHI when feasible. If infeasible, protections continue and further use or disclosure is limited to the purposes making return or destruction infeasible. [8] Document retained copies, restrictions, access, expiration, and the approved exit plan.

Price the approved clinical workflow

Price the selected voice workflow together with its storage, recovery, audit capability, training, account administration, vendor review, and incident coordination. Identify which tasks are retained by the practice and which are purchased. Compare bids for the same approved scope; a lower base price does not establish a lower complete cost when needed services or operating work are excluded.

HIPAA-COMPLIANT HOSTING

Hosting 3CX in a HIPAA-compliant data center costs more. Ask SPARK VoIP for HIPAA-compliant hosting pricing.

Table 4. Cost and evidence fields for a practice purchase

Budget category	Scope to price	Acceptance evidence
Voice platform	Users, devices, numbers, and carrier	Calling and route tests
Protected records	Voicemail, recording, and archive	Access, retention, and retrieval tests
Approved destinations	Email, records software, and integrations	Data map and destination controls
Governance	Risk review, BAAs, operating evidence, and staff procedures	Contracts, evidence scope, and assigned owners
Recovery and exit	Backups, outage retrieval, preservation, and export	Tested retrieval and termination process

Original cost collection framework. It asserts no national compliance price. Include the provider and records work described in Tables 2 and 3.

Compare no-recording and selective-recording workflows before approving capture of every call. A live call followed by an approved clinical note may meet the need with fewer copies; test it against actual clinical and records duties. No-recording still leaves possible voicemail, call logs, and clinical notes to assess. Transmission safeguards and provider roles still matter. Recording consent is a separate legal question.

Separate subscription charges from internal operating labor. If the provider performs account reviews or recovery tests, state the frequency and deliverable in the contract. If the practice retains those tasks, name the person and include the time in the comparison.

SEPARATE SCOPE

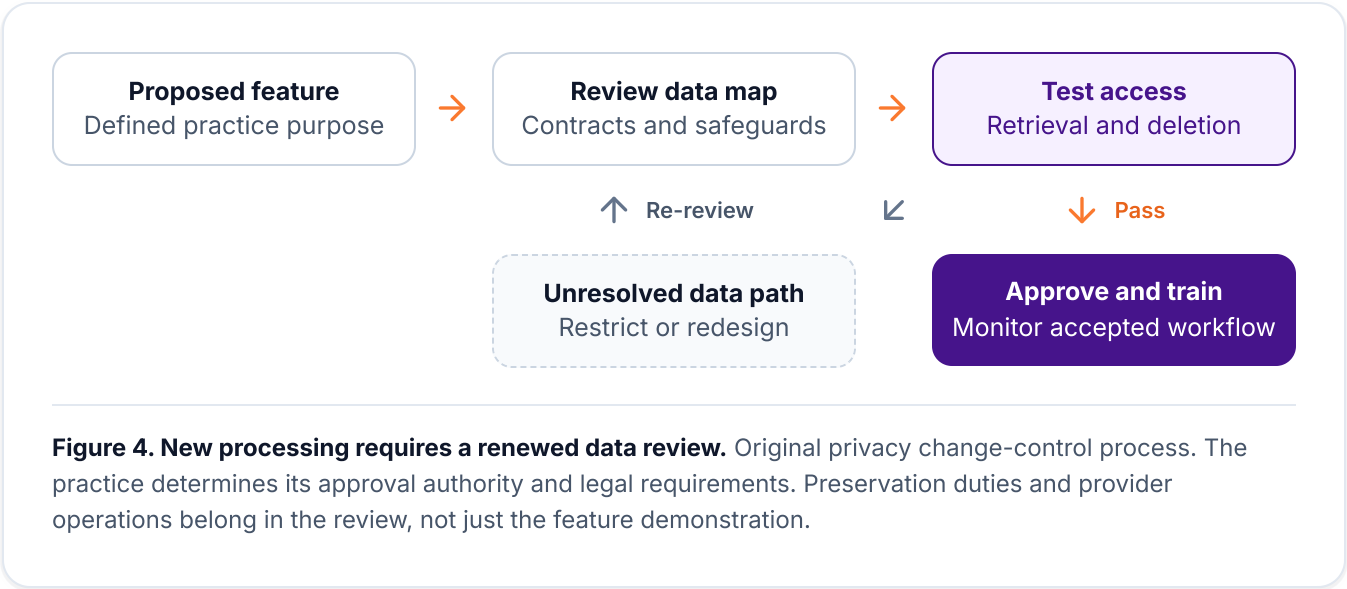
Veterinary practices

For veterinary practices, price owner-contact privacy, account security, payment handling, records confidentiality, and recovery on their own merits. Animal-only treatment data is outside the human-health premise used here; this is a scope inference. A practice handling human PHI for a covered entity, or operating another regulated service, needs separate assessment. [6]

09

Approve features through a privacy review

Treat each new sharing or processing feature as a data-flow change. Before activating a transcript, message integration, or automated summary, determine the receiving service, its access, the agreement, the retention, and the intended user. Staff should receive a clear permitted-use procedure.



Demonstrate a callback, authorized and unauthorized voicemail access, staff departure, readable export, archive retrieval, and recovery after a failure using approved synthetic data. Include loss of the provider's normal portal or hosting environment. Define who can obtain the retained records, by which method, and within the agreed recovery target; retain witnessed results.

At staff departure, revoke access and preserve records under the approved schedule and any applicable hold. Review shared mailboxes, forwarded voicemail, mobile sessions, and local copies. Removing the private branch exchange (PBX) account does not prove exported files or backup copies have been removed; track each destination separately.

Review provider and material feature changes. Retain the accepted configuration, data map, contract chain, operating-evidence register, and disposition schedule with the practice's risk records. Assign review owners and triggers. An installation test is one checkpoint, not proof of continuing control performance.

10

Approve patient data destinations

Use synthetic data to test access, revocation, export, preservation, and deletion in each destination. Pair the results with operating evidence from Table 2 and the record schedule in Table 3. Feature demonstrations do not establish patching discipline, incident handling, or continuing privileged-access control. These are recommended acceptance practices, not a universal certification checklist.

Table 5. Patient data destinations and approval evidence

Destination or feature	Evidence to request	Practice decision
Stored voicemail	Provider role, applicable BAA, access, preservation, and disposition tests	Approve the covered workflow
Voicemail email	Receiving account controls and attachment destinations	Choose attachment, link, or restricted access
Mobile application	Lost-device process, sessions, local copies, staff departure	Approve managed access conditions
Recording or transcript	Purpose, approved users, processor chain, clinical accuracy review, and record schedule	Limit capture to approved needs
Backup and archive	Outage restore test, hold handling, expiration cycle, and re-deletion after restore	Set recovery and retention responsibilities
Provider exit	Readable export, continued access, return or destruction, and infeasibility handling	Accept a practical exit plan

Original recommended working matrix. Assign names and record actual evidence before approving the purchase.

Classify features as approved, restricted pending evidence, or excluded. Contract coverage, destination access, provider operations, and record preservation are separate approval questions. A missing BAA for a maintained-ePHI service cannot be resolved by an access demonstration. Record the owner, evidence, unresolved gaps, and decision before the workflow goes live.

Make the decision from workflow evidence

HISTORICAL ENFORCEMENT CONTEXT

Oregon Health and Science University settlement

\$2.7M **JUL 18, 2016**

settlement

HHS announcement

HHS announced a \$2.7 million settlement with Oregon Health and Science University (OHSU) on July 18, 2016, addressing potential Privacy and Security Rule violations and broad safeguard failures. This institutional case supplies historical context; it does not measure a small practice's phone-system risk, establish a penalty per call, or forecast a fine. [5]

A hypothetical dental group may choose a secure hosted voicemail platform and still email recordings to an unmanaged personal inbox. The relevant procurement gap is the destination and access workflow. Buying another encryption feature on the server would leave that gap unresolved.

Purchasing decision

Walk through an approved interaction from receipt to retrieval, preservation, and final disposition. Require the data map, contracting chain, operating evidence, and witnessed tests. Review separately purchased services directly; ask the phone provider to document its own downstream obligations. Compare selective capture and no-recording options before expanding the archive.

Treat transcription and automated summaries as proposed processing capabilities. Before clinical adoption, test errors, omissions, speaker attribution, routing, and correction on representative approved tasks; record accuracy and reviewer workload. No measured practice benefit or accuracy result is supplied here. Require an accountable reviewer, approved record-entry process, data purpose, access controls, retention, and appropriate agreements.

A defensible decision

A defensible decision requires a documented scope, evidence, responsible owners, and a plan for unresolved risks.

Ask SPARK VoIP to demonstrate the approved safeguards and operating controls in your pilot and confirm the service scope in the written proposal. Review the signed BAA together with the workflow and witnessed results.

References

Numbered references support factual and regulatory statements. Recommendations and original frameworks are identified in the text. Sources checked October 4, 2026. Current eCFR pages used here display Title 45 through October 1, 2026; guidance dates are stated where established.

- [1] HHS Office for Civil Rights. Covered Entities and Business Associates. Applicability and electronic standard transaction criteria.
[Read source](#)
- [2] HHS Office for Civil Rights. Guidance on HIPAA and Cloud Computing. Business associate storage relationships, encrypted data, and conduit distinction.
[Read source](#)
- [3] HHS Office for Civil Rights. Guidance on Audio Only Telehealth. Content reviewed June 23, 2026. Transient conduit roles, maintained data, and BAA analysis; applied to the described service behavior.
[Read source](#)
- [4] HHS Office for Civil Rights. Summary of the HIPAA Security Rule. Current safeguards and required versus addressable specifications.
[Read source](#)
- [5] HHS Office for Civil Rights (July 18, 2016). Oregon Health and Science University settlement and corrective action plan.
[Read source](#)
- [6] 45 CFR 160.103. Definitions of health information, PHI, covered entities, and business associates. Text read on Cornell Law School's Legal Information Institute after direct eCFR retrieval was blocked. Veterinary applicability is a scope inference.
[Read source](#)
- [7] Office of the Federal Register. 45 CFR 164.308. Administrative safeguards. Sections (a)(1), (a)(6)–(8), and (b); risk, incident, contingency, and direct versus downstream assurances. Current eCFR text checked October 4, 2026.
[Read source](#)
- [8] Office of the Federal Register. 45 CFR 164.504(e). Business associate contracts, permitted uses, subcontractor commitments, and termination return or destruction with infeasibility protections. Current eCFR text checked October 4, 2026.
[Read source](#)
- [9] HHS Office for Civil Rights. Medical record retention FAQ. Privacy Rule distinction from medical-record retention requirements; safeguards continue through disposal. Checked October 4, 2026.
[Read source](#)
- [10] Office of the Federal Register. 45 CFR 164.316(b). Security Rule documentation and its six-year retention measure. Current eCFR text checked October 4, 2026.
[Read source](#)
- [11] HHS Office for Civil Rights. HIPAA Security Rule NPRM. Proposed rule announced December 27, 2024. Agency page states that the current Security Rule remains in effect during rulemaking; checked October 4, 2026.
[Read source](#)

Methodology and research limits

Research prioritized HHS guidance and the enforcement record, with current eCFR sections on administrative safeguards, contracts, and documentation. Cornell supplied the definitions after the direct eCFR page was blocked. The veterinary distinction is an inference about human-health scope. Diagrams, budget and evidence matrices, disposition practices, and acceptance procedures are original recommendations rather than validated compliance instruments.

This paper gives procurement guidance, not a legal opinion or seller certification. It does not cover every state privacy or retention law, substance-use record duty, or clinical telehealth rule. Confirm the service agreement, provider risk assessment, and operating evidence for the proposed scope. Test encryption boundaries, availability, recovery, deletion, and automation performance in the practice's pilot. The enforcement example is historical; proposals are not treated as enacted duties.

Evidence gaps

Obtain the entity-role assessment; risk analysis; actual BAAs and downstream responsibilities; processing inventory; provider patching, access, incident, and recovery evidence; approved record schedule and hold process; encryption boundaries; access-event logging; and witnessed export and disposition tests. A provider claim or one interface demonstration cannot answer these deployment questions. Practice counsel or a records specialist should assess applicable preservation duties.

Figures and tables

Figure 1	One conversation can create several retained records
Table 1	Provider roles and questions for contracting
Figure 2	Direct and downstream agreements follow the service relationship
Figure 3	A secure server is only one part of the control chain
Table 2	Provider operating evidence for the proposed service
Table 3	Record retention and disposition planning matrix
Table 4	Cost and evidence fields for a practice purchase
Figure 4	New processing requires a renewed data review
Table 5	Patient data destinations and approval evidence

Publication context

SPARK VoIP provides a 3CX based hosted voice over Internet Protocol (VoIP) offering. This paper is educational and does not establish a contract, legal opinion, certification, or guaranteed result. Service scope, support, integrations, and any regulated workflow need written confirmation for the proposed deployment.



Talk to SPARK VoIP

SALES

(888) 223-1094

SUPPORT

(918) 608-8888

WEB

sparkvoip.net

Emergency support is available 24/7.