Adaptive Business Continuity for HIPAA Manifesto

Adaptive Business Continuity for US Health Care Organizations

Authored by Sean Huggans, Adam Thomas, and Jose Medina

With thought contributions from Ed Finley, retired hospital administrator

Based on Adaptive Business Continuity methodology by David Lindstedt, Ph.D. and Mark Armour

This work is independently authored and is not affiliated with, endorsed by, or officially representing David Lindstedt, Mark Armour, or the Adaptive Business Continuity project. ABC HIPAA is an independent framework that builds upon and extends ABC methodology for regulated health care environments.

Note for readers: This framework uses ITIL (Information Technology Infrastructure Library) terminology as the standard for IT service management. ITIL provides common language for health care organizations to communicate about technology components and dependencies. Technical terms are explained throughout for clinical staff, administrators, and executives.

The Problem

US health care organizations are trapped between regulatory requirements and operational reality. HIPAA Security Rule requires risk analysis and contingency planning, including disaster recovery and emergency mode operation procedures. Traditional business continuity (BC) approaches respond with massive documentation projects that are costly and can consume months or even years of time, if ever being completed at all, while providing no actual protection.

Many health care organizations know WHAT they need to do for HIPAA compliance - but they are lost on HOW to do it practically.

Rural hospitals understand they need disaster recovery plans, but how can a 1 or 2 person IT team create actionable procedures while also taking calls about printers and resetting passwords? Large health systems know they need risk assessments, but how do you avoid six-month documentation projects that produce shelf-ware? These organizations all recognize they need disaster recovery capabilities, but how do you build real protection within limited budgets?

This creates a dangerous gap: compliance theater that satisfies auditors while leaving real systems vulnerable.

Rural health care organizations face these challenges with particular intensity - IT teams of 1-3 people managing entire hospital infrastructures, limited budgets competing with patient care needs, and geographic isolation from vendor support. But the problem affects all US health care: when compliance becomes documentation instead of capability, patients and operations remain at risk.

Traditional BC methodology demands completion of extensive, and largely hypothetical, risk assessments and business impact analyses before any protective work can begin. In 2017, David Lindstedt and Mark Armour published Adaptive Business Continuity (ABC) - a methodology that challenged everything traditional BC got wrong. ABC replaced massive documentation projects with concise reference materials intended to support trained responders. It shifted organizations away from pass/fail plan validation and toward

continuous capability improvement. It emphasized practical recovery planning benchmarks over rigid target-setting detached from operational reality. And it said what practitioners had been thinking for years: drop the traditional risk assessment and business impact analysis entirely. Stop producing shelf-ware. Start building actual recovery capabilities.

For most industries, ABC is the answer.

For US health care, it is an answer you cannot fully use - and for good reason.

This is health care, not a donut shop. HIPAA Security Rule requires risk analysis because patient data demands it. It requires contingency planning because lives depend on system availability. These are not bureaucratic overreach - they are reasonable expectations for an industry handling the most sensitive data in existence. Health care organizations cannot simply choose to skip risk assessment; it is federal law, as it should be.

The problem is not that HIPAA requires these things. The problem is that neither available methodology can satisfy those legitimate requirements practically. The very thing pure ABC tells you to omit, HIPAA rightly tells you that you must do. And the traditional approach that does satisfy the requirements buries organizations in documentation that provides little to no actual protection during real incidents.

The problem is accelerating. HIPAA requirements are under active regulatory pressure to become stricter and more numerous - for both covered entities and business associates. HHS has proposed changes that would make the Security Rule significantly more prescriptive, and specifications previously classified as addressable - meaning organizations could implement alternatives with documented rationale, though some simply treated them as optional - are proposed to become explicitly required. Whether or not every proposed change becomes final, the regulatory direction is clear. Organizations that build capabilities ahead of these changes will be positioned; those waiting to react will be scrambling. The total compliance burden is growing, and it competes for the same limited staff time and/or budget that disaster recovery planning needs. A methodology that advances multiple compliance requirements simultaneously through a single effort - which CI (Configuration Item) mapping does - is simply a wise approach to an overwhelming problem.

And the traditional approach allows something that should be impossible: producing a "compliant" disaster recovery plan without ever involving the people who would actually execute it. Organizations have produced disaster recovery plans without asking IT a single question about how systems are configured, connected, or recoverable. Others dump disaster recovery planning entirely on IT without any clinical or operational involvement.

Both failure modes produce documentation that cannot support actual recovery - which is the clearest evidence that the traditional approach values the document over the capability.

The Solution: ABC HIPAA Framework

ABC HIPAA synthesizes Adaptive Business Continuity methodology with HIPAA regulatory requirements using the "neo-compliance" approach: fulfill HIPAA requirements efficiently through practical implementation, not bureaucratic documentation.

ABC HIPAA was developed specifically because pure ABC methodology cannot work in regulated health care environments. HIPAA mandates certain documentation and risk assessments that cannot simply be omitted. The solution is not to abandon ABC principles, but to apply them to HOW you fulfill regulatory requirements.

ABC HIPAA provides the practical "how" framework for health care organizations lost between knowing WHAT they need to do for HIPAA compliance and HOW to actually implement it within real-world constraints. The framework stands on four assumptions that shape every recommendation that follows.

Framework Cornerstones

These foundational assumptions underpin the entire ABC HIPAA methodology. They inform how every element of the framework should be understood, applied, and evaluated.

Cornerstone 1: The Competence Assumption

ABC HIPAA documentation assumes that the person executing procedures is reasonably competent in the relevant domain. It does not attempt to substitute for professional competence, training, or appropriate staffing.

If someone with no competence in the relevant domain picks up ABC HIPAA documentation and fails to execute it successfully, that is a staffing problem - not a framework failure.

The Competence Threshold Test: "Could a competent professional who is new to this organization successfully use this documentation?"

Cornerstone 2: The Standalone Deliverable Requirement

ABC HIPAA documentation must function as a standalone deliverable that can be handed off and used independently. It cannot assume the creator will be present to explain, interpret, or supplement the documentation.

The Handoff Test: "If the person who created this documentation disappeared tomorrow, could someone else pick it up and use it successfully?"

Cornerstone 3: Capability vs. Documentation Accountability

The ABC HIPAA framework delivers a methodology for building documentation and capabilities. It does not guarantee organizational outcomes.

The framework provides the tools. The organization must do the work.

The framework maximizes the probability of success. It cannot guarantee success (and truthfully, no framework can).

Cornerstone 4: Regulatory Compliance (Neo-Compliance)

ABC HIPAA is designed to satisfy HIPAA Security Rule requirements, not circumvent them. The framework applies ABC principles to HOW organizations fulfill regulatory mandates, not WHETHER they fulfill them.

We fulfill HIPAA requirements. We do not circumvent them.

The answer is neo-compliance: ABC principles inform HOW you satisfy regulatory requirements, not WHETHER you satisfy them.

ABC HIPAA treats all HIPAA Security Rule specifications as required, including those historically labeled "addressable." Addressable never meant optional - it meant organizations must implement the specification OR document why an alternative provides equivalent protection. This is a deliberate framework methodology choice. Current HIPAA regulations still distinguish between required and addressable specifications. However, HHS has proposed changes that would eliminate this distinction, and treating everything as required now positions organizations ahead of that regulatory direction regardless of whether the proposed changes become final - now or in the future.

This methodology allows teams an efficient method to operationalize key Security Rule requirements while gaining real protection - something that increased regulatory scrutiny is at its root intended to accomplish. Traditional BC methodologies respond to regulatory pressure with additional busy work that provides no additional protection; ABC HIPAA responds by building actual capabilities that support compliance efficiently.

PHI Protection Continuity

Strip out the PHI protection thread, and ABC HIPAA becomes a perfectly good IT disaster recovery methodology for any industry. What makes this specifically a health care framework is the regulatory obligation to protect patient health information during every phase of operations - including the phases where normal systems and controls are unavailable.

HIPAA does not pause during outages.

During normal operations, ePHI protection is handled by technical controls: access controls, audit logs, role-based permissions, encryption. When systems go down, those controls go down with them. The organization does not get a compliance holiday.

In many post-incident reviews, the hardest control failures emerge during and immediately after the incident itself: emergency access granted but never revoked, break-glass account usage never reviewed, paper records created during downtime not secured appropriately, no audit trail for actions taken during the emergency period. These are the predictable consequences of not planning for PHI protection during the exact moments when protection is hardest to maintain.

PHI Protection Continuity is operationalized through four safeguard domains applied to every CI in the framework: **Emergency Authorization** (who can authorize emergency access and how), **Minimum Necessary Scope** (what access is permitted and what is not), **Manual Logging Requirements** (what must be recorded, where, and by whom), and **Post-Restoration Reconciliation** (how emergency-period activity is reviewed after restoration). Structure is uniform across every CI. Content varies - CIs with ePHI impact carry substantive procedures; CIs without ePHI impact carry a documented N/A determination that confirms the assessment was made.

PHI Protection Continuity is the health care differentiator, not the DRP scope limiter.

The framework's disaster recovery planning scope encompasses the entire CI inventory. PHI Protection Continuity adds a layer of additional rigor for systems that store, transmit, or gate access to ePHI. It does not define the boundary of what gets recovery planning; it defines which CIs require the four safeguard domains to carry substantive procedures.

The Neo-Compliance Philosophy

Create abbreviated compliance documents quickly, then focus time on building actual recovery capabilities.

A single comprehensive CI mapping effort satisfies multiple HIPAA requirements simultaneously - ePHI system inventory, risk analysis, contingency planning, emergency mode operations, emergency access procedures, disaster recovery planning, criticality analysis, audit controls, and information system activity review. The organization builds one set of documentation that works both operationally and for compliance.

The Security Rule requires a Risk Analysis of all ePHI to identify risks and vulnerabilities. You cannot perform that analysis without first knowing every system that stores, transmits, or processes ePHI. It is the position of this framework that a complete CI inventory is a highly defensible operational method for satisfying that requirement, and the basis of thorough contingency and recovery planning.

ABC HIPAA satisfies the risk analysis requirement through two complementary deliverables: a global **Threat and Vulnerability Context** document that identifies reasonably anticipated threats organized by effect category with likelihood ratings, and the **CI documentation set** that captures per-system vulnerability, impact, and risk treatment through dependency mapping. Together these constitute a complete risk analysis without the redundancy of repeating overlapping threat analysis for every system. The analytical effort focuses on actual system relationships and real organizational vulnerabilities rather than theoretical threat enumeration.

ABC HIPAA Principles

Principle 1: Start with Crown Jewels, Build Incrementally

Traditional Approach: Document everything before protecting anything.

ABC HIPAA Approach: Identify your 3-5 most critical clinical applications. Map their dependencies completely. Protect them thoroughly. Expand systematically. This is the Crown Jewel Fast Track.

Crown Jewel designation serves three simultaneous purposes: as a **scoping mechanism** that prevents paralysis by focusing effort on 3-5 systems, as a **learning mechanism** where the organization masters the methodology on manageable scope, and as **infrastructure coverage by proxy** because dependency mapping of Crown Jewels pulls in approximately 80% or more of core infrastructure automatically.

Crown Jewels are clinical applications that directly deliver patient care, not infrastructure. Crown Jewel status is determined by whether loss of the system causes **operational**

paralysis or **operational degradation**. Systems that cause paralysis are Crown Jewel candidates.

This is not "do minimal work now, circle back later." This is "do complete CI dependency mapping on limited scope, then expand complete methodology to additional systems," making progress on manageable chunks thereafter.

HIPAA Reconciliation: Crown Jewel identification satisfies HIPAA applications and data criticality analysis requirements while delivering immediate focused protection.

Principle 2: Complete the Circle, Do Not Create It

Traditional Approach: Defer complexity to "Phase 2" that never happens.

ABC HIPAA Approach: HIPAA requires risk analysis of all ePHI systems. A comprehensive CI inventory is the most defensible way to identify what those systems are and how they interconnect. Complete full CI/dependency mapping to enable compliant risk analysis.

Sean's Philosophy: "Do It Right, Instead of Right Now"

"Circle back" is a lie in resource-constrained organizations. PHI systems likely depend on infrastructure, network, authentication, and storage systems that comprise 80% of your total IT environment. Complete comprehensive IT/CI mapping to enable thorough risk analysis rather than creating deferred work that will never happen.

The scope of disaster recovery planning encompasses the entire CI inventory, not exclusively systems handling PHI. Dependency mapping makes this self-evident - when you document the dependencies of your Crown Jewel EHR, you discover it depends on Active Directory, core switches, SAN storage, DNS, and WAN circuits. None of these store patient records. All of them are essential to the EHR's availability. This is not scope creep - it is the natural result of dependency mapping.

ABC HIPAA uses a five-part CI documentation structure: CI Information (what is this thing), Contingency Plan (what does business/clinical do while it is down), Recovery Plan (what does IT do to restore it), Upstream Dependencies (what does this CI depend on), and Downstream Dependencies (what depends on this CI).

HIPAA Reconciliation: The CI inventory serves as the technical foundation for multiple HIPAA requirements - risk analysis and contingency planning built on the same foundation, supporting the "living document" mentality of ABC rather than static annual refresh cycles.

Principle 3: Document for Memory, Not Auditors

Traditional Approach: Create comprehensive plans that staff will feel too overwhelmed to use in a panic during real incidents.

ABC HIPAA Approach: Create mnemonic documents that remind trained staff of practiced procedures.

Documentation exists to support trained responders, not replace training. Health care staff must deeply understand their roles during system failures at an instinctive level - not from reading a binder, but from having developed and practiced their response. Documents serve as reference points for processes staff have already internalized, not instruction manuals for complex procedures.

HIPAA Reconciliation: Required contingency plan documentation focuses on actionable procedures that support actual response capabilities, satisfying regulatory requirements through useful deliverables.

Principle 4: Exercise for Improvement, Not Testing

Traditional Approach: Annual exercises that test whether plans work.

ABC HIPAA Approach: Regular exercises that improve response capabilities and identify gaps.

Testing implies pass/fail. Improvement implies continuous development. Health care systems change constantly - new technologies, workflows, staff, regulations. Capability improvement exercises reveal gaps in real time and build competency.

Every exercise program should include scenarios where key personnel are unavailable. Personnel single points of failure are common, especially in rural health care organizations with small IT teams. These scenarios frequently reveal gaps. That is the point.

HIPAA Reconciliation: Required testing and revision procedures focus on continuous improvement rather than validation, satisfying HIPAA requirements while building actual preparedness.

Principle 5: Realistic Recovery Objectives Over Rigid Targets

Traditional Approach: Assign precise RTO/RPO targets based on business impact assessments, then treat them as contractual commitments.

ABC HIPAA Approach: Define recovery objectives as realistic planning benchmarks informed by actual operational constraints, not rigid commitments that ignore incident variability.

Recovery objectives include Recovery Time Objective (RTO) as a planning benchmark, Recovery Point Objective (RPO) driving backup frequency, and Maximum Tolerable Period of Disruption (MTPD) as the absolute outer boundary representing hard restrictions that cannot be negotiated - regulatory deadlines, life safety dependencies, and contractual SLA requirements. RTO is what you plan for. MTPD is what you cannot exceed.

Recovery objective values should reflect actual operational constraints, not aspirational targets. Plan for immovable restrictions. Adapt everything else based on actual incident conditions.

HIPAA Reconciliation: Focus on regulatory deadlines and patient safety requirements as true restrictions rather than artificial recovery time targets.

Principle 6: Fulfill Requirements Through Capabilities

Traditional Approach: Create documentation that auditors want to see.

ABC HIPAA Approach: Build capabilities that HIPAA actually requires, documented appropriately.

Satisfy HIPAA requirements through practical implementation that creates real protection, documented to support actual capabilities.

HIPAA Reconciliation: Every required HIPAA safeguard becomes a measurable capability, not a checkbox item.

Principle 7: Measure Capabilities, Not Documents

Traditional Approach: Count completed plans, exercises performed, refresh dates maintained.

ABC HIPAA Approach: Measure and benchmark actual recovery capabilities over time.

The final measure of preparedness is effective response and actual recoverability. Three factors define recovery capability (RPC Model): **Resources** (degree to which recovery resources will be available when needed), **Procedures** (degree to which each responder knows and has internalized their disaster role), and **Crisis Competencies** (degree to which responders can function effectively throughout incident duration).

The framework identifies personnel single points of failure as measurable findings - not to assume organizations can eliminate them, but to give leadership visibility into the risk. That visibility is progress.

Establish baselines early and measure improvement over time.

HIPAA Reconciliation: Required evaluation procedures focus on measuring actual security and recovery capabilities rather than documentation compliance.

Principle 8: Engage IT and Clinical Operations Together

Traditional Approach: IT creates technical recovery plans in isolation.

ABC HIPAA Approach: IT and clinical operations develop integrated response capabilities.

Health care recovery requires coordination between IT restoration and clinical workflow adaptation. Real incidents involve two parallel tracks: the **Contingency Track** (what clinical and business staff do while systems are unavailable) and the **Recovery Track** (what IT does to restore service).

Traditional BC often treats these tracks in isolation - or worse, excludes one entirely. ABC HIPAA's CI-driven approach makes this structurally impossible: you cannot build the CI inventory without IT, and you cannot build contingency plans without operations. The methodology forces the engagement that traditional approaches allow organizations to skip.

ABC HIPAA connects the tracks through the **Contingency Handoff** - a structured coordination point where IT communicates scope, timeline, and contingency activation recommendations to operations before beginning focused recovery work. This handoff includes a critical **Quick Helps Window** where IT can provide time-sensitive assistance (printing patient census, exporting medication records) before diving into troubleshooting.

Pure ABC methodology places primary emphasis on escalation to IT, which is insufficient in health care environments where clinical downtime procedures must also be pre-built. ABC HIPAA builds both contingency and recovery plans on the same CI inventory foundation. Both must exist before an incident occurs.

HIPAA Reconciliation: Integrated planning ensures contingency procedures address both technical recovery and clinical workflow continuity required to maintain ePHI availability.

Principle 9: Prepare for Effects, Not Causes

Traditional Approach: Identify specific threats and plan responses to each cause.

ABC HIPAA Approach: Build capabilities to respond to the effects any incident produces on your IT environment.

Every disaster produces effects. The cause (tornado, ransomware, power surge) provides context, but the response capabilities needed are determined by the effect, not the cause. Cause-based planning has a fatal gap: when something you did not plan for happens, you

have no plan at all. Effect-based planning covers threats you have not imagined yet, because the effects on your environment are the same regardless of what caused them.

Pure ABC methodology identifies three fundamental effects: unavailability of location, unavailability of people, and unavailability of resources. For health care organizations, the ABC HIPAA framework expands these into nine effect categories: Loss of Facility Access, Loss of Power/Utility Services, Loss of Network Connectivity, System or Application Failure, Cyberattack/Pervasive Malware, Unauthorized Access/Data Breach, Vendor/SaaS Provider Outage, Data Loss or Corruption, and Loss of Key Personnel.

HIPAA Reconciliation: Effect-based planning ensures contingency procedures address all potential ways ePHI systems might become unavailable, regardless of specific causes. The nine effect categories provide structured threat identification without exhaustive threat enumeration.

Principle 10: Continuous Improvement Over Annual Refresh

Traditional Approach: Annual plan updates and exercise cycles.

ABC HIPAA Approach: Ongoing capability improvement based on operational changes and lessons learned.

Health care organizations change constantly: new systems, workflows, regulations, staff. Annual refresh cycles cannot keep pace with operational reality. Integrate BC improvement into normal IT operations. When systems change, update recovery capabilities immediately. When exercises reveal gaps, address them before incidents test them.

HIPAA Reconciliation: Required periodic evaluation occurs continuously through operational integration rather than artificial annual cycles.

Implementation Philosophy

Crown Jewel Fast Track

Focus to learn, not defer to circle back. Begin with your 3-5 most critical clinical applications, complete full CI inventory and DRP processes (contingency plans, recovery plans, and emergency mode safeguards), measure and demonstrate recovery capabilities, then expand the proven methodology to remaining systems.

Crown Jewels receive the same complete documentation you would do for the full environment - you are just limiting the initial scope to learn the methodology while delivering immediate value.

Business Associate Continuity Verification

HIPAA requires covered entities to obtain satisfactory assurances from business associates that ePHI will be appropriately safeguarded, formalized through written contracts meeting 45 CFR 164.314(a). ABC HIPAA's recommended approach includes vendor questionnaires, shared responsibility matrices, regular capability verification, and contract requirements ensuring BAAs explicitly address business continuity.

Vendor questionnaires must be short enough to actually get completed. Short-form questionnaires focused on the questions that matter get completed and provide actionable data. SOC 2 reports should be accepted as supplemental evidence, not substitutes for specific answers about how vendor capabilities support your recovery objectives.

Resource-Appropriate Implementation

The framework scales from critical access hospitals to major health systems, with phased implementation that builds standalone value at each step and special attention to the multi-hat reality of rural health care IT staff.

Call to Action

US health care organizations deserve disaster recovery planning that protects patients, staff, and operations while satisfying regulatory requirements. HIPAA compliance should enhance security through practical capabilities, not create documentation burdens that divert resources from patient care.

The gap between compliance theater and operational reality puts communities at risk. Rural health care organizations especially cannot absorb the costs of this gap - limited resources demand maximum protection from every IT investment.

Stop accepting the false choice between compliance and capability. Stop being lost in the "how." Start building adaptive, practical, sustainable health care preparedness.

Begin with Crown Jewel identification. Build real capabilities. Document appropriately. Expand systematically.

Designed for the resource constraints and geographic realities of rural health care, applicable across all US health care organizations committed to practical preparedness over compliance theater.

Legal Disclaimer

This manifesto provides methodological guidance for HIPAA compliance approaches but does not constitute legal advice. HIPAA enforcement actions by the Office for Civil Rights (OCR) are highly individualized, taking into account factors such as organizational size, complexity, good-faith compliance efforts, and the specific circumstances of any incident or audit. Organizations should consult qualified legal counsel familiar with health care privacy law for compliance guidance specific to their situation and operational environment.

The ABC HIPAA methodology is designed to satisfy regulatory requirements through practical implementation, but each organization must evaluate its own risk tolerance and compliance needs in consultation with appropriate legal and compliance professionals. Use of this framework does not by itself establish HIPAA compliance. Security Rule compliance depends on each organization's specific environment, safeguards, documentation, and implementation.

ABC HIPAA is a pending trademark of VISUAFUSION LLC. Use of the ABC HIPAA name to describe or reference this framework is welcomed and encouraged. Use of the ABC HIPAA name to brand, market, or imply affiliation for other organizations' products or services without authorization may constitute trademark infringement.

References

Lindstedt, David and Mark Armour. Adaptive Business Continuity: A New Approach. Rothstein Publishing, 2017.

Lindstedt, David and Mark Armour. "Adaptive Business Continuity Manifesto." Originally published September 15, 2015; updated January 2017.

Jackson, Brian A. "The Problem of Measuring Emergency Preparedness: The Need for Assessing 'Response Reliability' as part of Homeland Security Planning." RAND Corporation, 2008.

Hubert, Rainer. "Why the Business Impact Analysis Does Not Work." The Business Continuity and Resiliency Journal, 1(2), 31-39, 2012.

National Institute of Standards and Technology. "NIST SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems." May 2010.

U.S. Department of Health and Human Services. "HIPAA Security Rule." 45 CFR Part 164, Subpart C.

U.S. Department of Health and Human Services. "Guidance on Risk Analysis." July 2010.