Capstone Project Summary and Reflections

My capstone project was a HIPAA compliance audit for a hospital implementing a Large Language Model (LLM) to process patient medical records. The goal was to create a "HIPAA-first" audit program for this AI system, meaning I let HIPAA's requirements drive the audit process from start to finish.

In the early phase of the project, I focused heavily on understanding and mapping all the required HIPAA safeguards – administrative, physical, and technical – in the context of the LLM.

In the process of understanding the HIPAA Security Rule and the Privacy Rule, I came across the SRA (Security Risk Assessment) tool from the HHS, designed for small to medium businesses to do a risk assessment (which is a core requirement of the HIPAA Security Rule).
The SRA is a very comprehensive assessment of the posture of an organization. You enter in your assets, locations, and partners, then it will prompt you before each section with a list of areas your organization may need to review, and based on that it will ask questions.

For example, Section 2: Security Policies.
Covers documentation and upkeep of your written policies.
Q6. How long are information security management and risk management documents kept?
And it gives you multiple-choice answers — one of them is:
"We maintain documents for at least six (6) years from the date of their creation or when they were last in effect, whichever is longer. These documents are maintained and backed up."
A education box pops up:
"This is the most effective option among those provided to protect the confidentiality, integrity, and availability of ePHI. The federal requirement is six (6) years retention of documentation, but your state or jurisdiction may have additional requirements."
And a list of references showing exactly which HIPAA and NIST requirements apply and whether they are required by HIPAA.
This tool covers all required and addressable HIPAA concerns, and it gives you a risk matrix of critical, high, medium, and low on all the main areas, which all those questions fall under.

It's a highly informative document — a Risk Control Matrix detailing the risks and controls and mapping them to the HIPAA requirements.

Deliverable #1: (SRA) Security Risk Assessment Report.

Then I created a PowerPoint to help non-technical listeners understand the principles of HIPAA without going into the details. I wanted the viewer to understand that HIPAA is not requiring specific technologies, and to understand the structure of the Security Rule — the difference between "required" and "addressable," the "appropriate and reasonable" principles, and the structure of the rule: administrative, physical, and technical safeguards.

Deliverable #2: HIPAA Security Standards

I also did a presentation on what the LLM would look like from the perspective of the hospital, and filled it with corporate jargon explaining the utility from a business perspective. I gave the hospital a name — Evergreen Valley Medical Center — and our fictitious security company I called Alexos Security LLC.

Deliverable #3: Patient-Care Open-Source-AI

After researching and understanding the HIPAA rules well, I started drafting the audit outline and began with an executive summary section, followed by an intended audience section, and a scope section (following the outline of a professional audit).

I addressed in the document some of the fundamental issues with using an LLM and a creative solution around it — namely, using de-identified data and piggybacking off the existing Electronic Health Record (EHR) system for access control.

Then a section to give the reader an understanding of HIPAA requirements and structure, with a matrix to help with understanding.
Then we got to the matrix where we mapped the HIPAA requirements — under which category they fall (e.g. administrative, physical, or technical), whether they are required or addressable, and the controls, sub-controls (e.g. the specific tech we assume the hospital would be using), the verification method we as auditors would look for, and finally a residual risk score — meaning after applying the control:

Deliverable #4: LLM Audit Project Draft

We then proceeded and did a specific LLM vulnerability matrix where we went through a list of very specific issues we assume a hospital implementing an LLM would face. This was the crux of the project — to create an audit program for the excess risk introduced by said technology.

The matrix works by mapping the business objectives to the risk and explaining why there is excess risk with a particular setup, the inherent risk (meaning before implementing controls), and then a very detailed control testing section where we outline how we as auditors would verify that those said controls are indeed implemented and effective, and a

residual risk rating — meaning after implementing the controls, how much risk we are left with.

Deliverable #5: LLM-Specific Risks Assessment

Finely I drafted a outline of an engagement letter between the hospital and Alexos Security LLC, which also follows the requirements of a BAA — Business Associate Agreement — required by HIPAA for all subcontractors working with PHI.

Deliverable #6: BAA agreement

I believe I delivered on all the project objectives.

Lessons Learned

I've learned so much during this process — and not just about HIPAA:

1. Research is important, but so is presentation.
2. A structured document with less content is worth a lot more than an unstructured collection of documents.
3. It is important to adhere closely to the defined project objectives (scope) and avoid falling into scope creep.
4. There are tools for almost anything like the very powerful RSA tool form the HHS