Appendix: Legal Defense of the Book
Patient Privacy for Small Clinics

These days, everything gets criticized. This book will be no exception. They will say it is "light weight", "not good legal advice." They will say it does not "cover all the possible situations." We are sure they'll say many other not-so-nice things. Here is our attempt to answer those questions before they arise. Note that in defending our approach, we criticize other HIPAA material.

Simple is Hard

Our approach was to decompose the complex HIPAA laws and reassemble them in approachable ways. We tried to hide the complexity behind familiar metaphors. Though we have tried to remove the legalese, there is a fair amount of legal scaffolding supporting the book's 8-step plan. As stated in the author bios, Kristen Ahearn is a nationally recognized subject matter expert in HIPAA and is the Privacy Officer at Memorial Sloan Kettering Cancer Center in NYC. (All of the author, who are in their mid-40s, live and work in the NYC area.) Kristen showed us what a robust privacy policy looks like and provided the legal scaffolding.

The authors worked together to find a middle ground that has on one extreme a robust patient privacy policy and on the other extreme the stark realities and resource challenges of a small clinic. Just making payroll is a bi-weekly challenge for many small clinics across America. It is not realistic to expect an office manager to find the quiet time to read a 300 page tome with references to CFR 45 § 160. blah blah blah….. Ain't gonna happen. This 8 Step Plan is the best we could do to find a middle ground.

We are wide open to suggestions, comments and feedback. And being New Yorkers, we are OK with harsh feedback. We get criticism everyday on the city sidewalks. You won't hurt our feelings.

(Update: we shortened this to 8 steps)

Our 10 Step Plan	**HIPAA Legal Relationship**
Assign a Privacy Officer	Basics
Create the Privacy Notebook	Basics - "Documentation"
Take An Inventory Of All Business Owned Equipment	Security Rule
Develop Policies & Procedures For "Patient Rights" Requests	Privacy Rule
Document Business Partners (e.g. Business Associates, Covered Entities)	Security Rule
Train The Clinic Staff In Patient Privacy	Privacy Rule, Security Rule

Take An Inventory Of Personal Equipment Used For Business Purposes (laptops, smart phones)	Security Rule
Monitor & Audit Staff Usage of Systems (e.g. Snooping in Medical Records)	Security Rule
Submit Breach Notifications	Breach Notification Rule
Provide On-Going Training	Basics

Some Other Thoughts
As we read through much of the existing HIPAA literature, we often made notes and had robust discussions about things we wanted to exclude. Perhaps this makes the book feel less legally authentic. But perhaps it makes it more readable for regular folks.

§ = ? (Or § Does Not Equal $)
Norby Ryan, the co-author who is a computer nerd, didn't even know what this symbol § meant. This was a role reversal because it is usually computer programmers that are having to explain all of their crazy computer symbols to other people. He has published in a technical journal, has a patent application, and 25+ years of professional computer experience, yet he didn't even know how to pronounce §. "Is it an emoji?" he thought to himself. He tried to Google it but even Google didn't have an answer. (Don't believe us? Try it: cut-n-paste just the symbol § into Google. Response: "Your search - **§** - did not match any documents.") Should we expect people working in a small clinic to know what § is?

In this book, we want to reach a wide audience. And, yes, we want to sell a lot of books! We feel that there is an inverse relationship between the number of times we use the symbol § and the number of books we sell. In general, people do not like to read things that confuse them. Time (and book sales) will tell if this theory is correct.

80/20 Rule
Another approach we used was to ask ourselves: Can we cover 80% of the law with a book 20% of the usual size? To achieve that end, one strategy we employed was to limit our scope. We focused only on small clinics. Therefore we ignored the perspective of health plans, researchers, big hospitals, health clearinghouses, and (sorta) patients. We chose sides; we are on the side of the doctor and Privacy Officer in a small clinic. It says it right there in our book title: "Patient Privacy for **Small Clinics.**" We are not trying to be everything to everybody. A second strategy we used, to get that 80%, is to make assumptions. We hope they are reasonable assumptions. There are a lot of abstract ideas in typical HIPAA documents. We avoided those abstractions and took a leap of faith by bright-lining some parts of the law. A good example of this is our simplification of who is or who isn't a Business Associate. Our third strategy was to be honest and upfront about only covering 80% of the law. We said, "this is just an introduction to HIPAA, HIPAA 101, you are gonna have to learn more, dive deeper,…."

We were not trying to be less-legally-correct (illegal? :), we are trying to communicate with regular people and we are trying to sell books. None of the authors is rich. We need the money and we don't want to be sued for giving bad advice.

HIPAA experts/lawyers will say how could you possibly leave out a discussion of X ?!?!?!? Our response is we want to connect with people and we want to sell books. When you talk about X, you don't connect with people and you don't sell books.

What is X? (Or some things that we purposely tried to avoid)
X = Covered Entity
Don't even know where to begin with that term. We weaseled out and said all clinics that see people-patients are "expected" to follow HIPAA. Yes, we know about the bit about "entities that electronically transmit any health information in connection with certain transactions…" nonsense - talk about weaseling out.

(Above we said "people-patients" because one small animal veterinary clinic in Texas has posted, on their website, a Notice of Privacy Practices direct from HHS. Still makes us laugh! Dying to go in there and request an accounting of disclosures for our dog.)

X = Security Rule versus Privacy Rule
Regular folks don't see the difference between security and privacy. "Aren't they the same thing?" they would say.

X = HIPAA, HITECH, NIST, CMS, NPP, PHI, EMR, OCR, HHS, CFR and countless other acronyms or abbreviations. How long does it take you to subvocalize all those acronyms? And you're an expert. Those acronyms are just as uncommunicative as §.

X = Risk Assessment
(Political rant coming) The regular folks think to themselves:

> "What the F do those jackwagon politicians know about risk assessments!?! Is that like when the Big Banks foreclosed on our homes then the government bailed out the Big Banks after they cut our retirement accounts in half? Should we use those risk assessments? Or should we use the risk assessment that said there were weapons of mass destruction in Iraq?"

These government regulations are onerous enough - now you want them to perform a poorly-defined risk assessment?? UUUGGGGHHH!!!

We would have liked to left out "Business Associate" too, but we kept that in.

Even "HIPAA" is debatable. Wish we had a nickle for everytime we read this paragraph:

"HIPAA, which stands for the Health Insurance Portability and Accountability Act, was signed into law in 1996…." blah blah blah.

Maybe it is not a good acronym if, every time it is is first used, you have to write a whole paragraph to explain the acronym. NASA, GE and IBM have huge marketing budgets and/or name recognition - HIPAA don't have that. We prefer "patient privacy." In fact, we prefer "foobar" or just about anything to HIPAA. Nothing makes us laugh louder than when very serious people spell it HIPPA. Maybe that's why the HIPAA Police are often portrayed as a hippo.

Seriously

There is nothing more serious than our health. And, spend enough time around clinicians, you'll find there is nothing more seriously funny. (Lawyers can occasionally be witty too.;) When you get so close to serious things, you need funny to survive. Nothing makes us LOL more than a lawyer and a doctor trading jokes about the other's profession. It is in that spirit that, throughout our book, we made some rather lame attempts at humor. Again, trying to be real and to connect.

So while we are familiar with those serious, legal sounding terms and concepts, we tried to hide or mask them behind approachable things like a "Privacy Notebook." Maybe it will work, maybe it won't.

If people start asking us (that's a big If) for the 20% of HIPAA that we didn't cover, then we'll recommend those 300 page serious-sounding-legal-HIPAA-tomes. Patient privacy and patient rights are worthy causes. Health care is a BIG BIG industry. Maybe there is room for both approaches.

To give us feedback, visit our Facebook page (need link) or tweet us #PatientPrivacyForSmallClinics or #PatientPrivacyTraining (need to set these up)