David Brooks of qliqSoft Talks to Us about Secure Communications, Replacing the SMS, and BYOD

Last week Mary Pat and I had a chance to meet and sit down for a while with a smart guy whose new venture is doing some really exciting things in the healthcare space. One of our favorite things to do! In an effort to keep on readers on the edge of what's new, and to give more of the people we meet a chance to say hello and connect to our audience, we present the first in the MMP Interview series.

We first got in touch with David when he commented on one of our 2.0 Tuesday posts on Medigram– a new, private beta secure communications service. David let us know that Medigram wasn't the only player in the space, and we agreed to meet for coffee and a chat. We got a chance to sit down with David soon after for a coffee and a demo of his company's flagship product qliqConnect– also currently in Beta.

David is a sharp, passionate guy, and we loved having the chance to talk to him. Check out the interview below!

MMP: I know that qliqSoft offers a secure method for healthcare communication – what exactly does that mean?

David: Technically, it means that our secure messaging application – qliqConnect – addresses 3 key areas of security necessary to support HIPAA/HITECH compliance, as well as satisfy guidance provided by the Joint Commission last

November: authentication, encryption and auditability.

In plain English, it means that qliqConnect allows all users within an organization (physicians, nurses, and staff) to participate in secure conversations using a variety of devices – computers (Mac & PC), laptops, tablets, and smartphones (iPhone & Android) – running familiar applications: texting on smartphones and chatting on computers. We've simply borrowed these phenomenally popular and successful consumer applications and integrated them into a single, secure communication platform that stands up to healthcares many rigors.

MMP: What is BYOD and how does that promote physician engagement with this technology?

David: BYOD stands for "bring your own device." It's a pretty basic idea that represents a sea change, not just in healthcare, but across many other industries in organizational attitude towards mobile devices. For years, conventional wisdom held that organizations could better secure and better manage devices if they standardized on a single platform and single device. In other words, the organization purchased the devices and issued them to employees. Think of Blackberry's golden years. While it is still arguably true that it is easier to secure and support a single device, the iPhone revolution proved that personally-liable (end-user owned) devices could not be kept outside of the work environment. Over the last couple of years, many organizations have moved away from the single-device approach and have instead sought ways to reign-in end-user devices.

At the end of the day, it is a trade-off. Organizations that accept a BYOD approach may give up a little control but should end up with higher end-user adoption, and in turn, higher productivity. Let's face it, who wants to carry around a second (typically inferior) device?

At qliqSoft, we are basically neutral on the subject of deployment models. I say “basically” because we are focused on supporting the platforms and the devices that end-users are using. Currently, we support iOS, so our application runs on iPhone, iPod Touch, and iPad. We are releasing Android in the next couple of weeks, and then we will begin working on a native iPad application soon after. We are not seeing enough demand on other platforms at this time to warrant the investment, but are always open to reassessing this.

MMP: We’ve heard a lot about HIPAA breaches recently – can you explain how qliqSoft protects patient information from being exposed on the internet or being accessed through lost or stolen laptops or smartphones?

David: I expect we’ll continue to hear about HIPAA breaches for quite some time. In fact, growing enforcement is driving many organizations to take a closer look at well-known gaps, such as SMS texting. Although we have developed a powerful and highly extensible secure communication platform, secure messaging is getting a lot of attention right now, as it should.

Our secure messaging solution, qliqConnect, addresses 3 primary security requirements needed to satisfy HIPAA/HITECH compliance, as well as guidance provided by the Joint Commission:

1) Authentication: our application requires end-users to log in using secure credentials.

2) Encryption: all data is encrypted both in transit and at rest.

3) Auditability: organizations have the option to store all message traffic on an organizational asset for archiving and audit purposes.

Additional security features include:

- remote lock and remote data wipe
- all messages are data/time stamped, along with message status (sent, pending, delivered/received)
- acknowledgement request to ensure message was received, read and understood by recipient

In addition to application features, it is worth mentioning a little about our architecture, as we do not employ a typical cloud-based client/server design. We do not store, nor can we access any of the information that flows through our network. All information is stored within customer resources (both smartphone and desktop computer clients). Although we utilize a cloud-based server to route message traffic in real-time, information is persisted in the cloud only long enough to complete message delivery, at which point it is deleted from our servers. The message traffic itself is encrypted using 1024-bit RSA encryption while attachments are encrypted using 256-bit AES encryption. Furthermore, all traffic is sent across port 443. The payload is encrypted using public keys and decrypted with private keys, which are locked inside end-user devices and clients. No one, other than the message recipient, can decrypt messages. In other words, storage is distributed and controlled by end-users and their organizations.

MMP: Who is your target market for qliqSoft – is it hospitals, or practices, or essentially all healthcare providers?

David: We believe that a secure communication solution must address all personnel in an organization, regardless of role and regardless the size of the organization. Everyone involved in patient care should have the opportunity to participate in secure conversations. Solutions that address only one set of constituents or that exclude key team members are of limited value and only contribute to healthcare IT's never-ending "silo-fication".

I should add that while there are no doubt opportunities to extend secure messaging into other industries, qliqSoft is a healthcare-focused company. Every aspect of our solution, from our platform with it's built-in HL7 integration engine to end-applications that support a number of healthcare-specific features, were designed to improve communications across healthcare.

MMP: How does qliqSoft compare with solutions already on the market?

David: For starters, we believe that our technology and our architecture provides superior security. For example, many larger organizations appreciate that we do not store all end-user traffic in a single cloud-based server. In addition to increasing the risk of a potential breach as well as the impact, centralized-storage places a tremendous burden on vendor organizations to properly manage stored PHI.

Nevertheless, I expect that most competitors in this space will offer credible answers to the requisite security questions. Increasingly I suspect conversation will evolve to the more fundamental question of usability. And, by "usability" I am not referring to minor features and functionality. Any vendor is capable of adding market-driven bells and whistles. I am talking about the most important question an end-user cares about: can I reach the people I need to?

Texting is a great application, but the reason SMS is the most popular application on the planet is because it doesn't require any special software. If you know someone's cell number, you can send them a text. Unfortunately, there is no way to secure SMS without introducing client-side software, at which point you would move away from SMS to superior technologies. The challenge then becomes how to build a secure solution that scales relatively easily so that end-users can reach the people they need to.

Although there is not a lot of discussion on this topic yet, I think it will quickly move to center-stage.

Unlike a number of our competitors that have deployed physician-only solutions, we have been inclusive of all healthcare professionals from day one. Additionally, we are getting ready to roll out a number of enhancements to our platform that will make it much easier for users to expand their secure network both within and beyond their direct organization.

MMP: If I gave this solution to my providers and staff, what immediate value can we expect? Longer term?

David: Honestly, if you gave your providers and staff qliqConnect, the most immediate benefit you would notice is that your compliance officer is sleeping better at night. I do not mean to minimize the value of qliqConnect or the potential it possesses. Rather, my point is to emphasize the degree to which people are currently abusing unsecure communication tools like SMS and chat. In other words, we are providing tools that your people are already using. And I hardly blame them. In an industry plagued by longstanding communication challenges, it only makes sense that healthcare professionals would turn to these great tools to improve workflow, and ultimately the care they provide. With qliqConnect, they can use these tools without fear and without looking over their backs.

Longer term there is no limit to the value users can gain. I mean that. Once we establish a secure connection between two individuals or two organizations, there are an infinite number of possibilities for exchanging both structured and unstructured data. In fact, most conversations I have these days start on the topic of secure texting and end on accountable care organizations (ACOs) and collaboratives.

MMP: What else does qliqSoft offer?

David: For the time being we are completely focused on making qliqConnect the best solution on the market. As I mentioned, we have a few exciting technical milestones coming up over the next couple of months, including support for Android as well as a number of enhancements to our underlying platform. Once those milestones are reached, we will resume work on both qliqCharge, our mobile charge capture application, as well as qliqCare, an enterprise-based variation of qliqConnect that expands functionality through integration with both clinical and telephony systems. Despite the incredible demand we have for additional tools and capabilities, we know that a laser-tight focus on our platform right now is going to pay huge dividends for qliqSoft and our customers going forward. These are exciting times for us.

Thanks so much to David for taking the time to show us qliqConnect and answer our questions!

You can learn more about qliqSoft at their website or follow them on Twitter