

## Web Portals

There are many traditional methods for transferring confidential data like email, online storage, mail, pickup, and an online service. But with the advent of increased bandwidth, more businesses are choosing to take their client's confidential data online. Putting client's data online comes with many challenges, and choosing the wrong solution can put your practice at risk. When considering options on the web, many hear words like web portals, horizontal portals, vortals, cloud computing, and SaaS. But with all these terms, it is increasingly difficult to navigate this sea of cryptic words and acronyms. It's important to understand how they all affect your business. This article will help you learn about new web technologies that will affect your choices and what that means for your clients' confidential data.

Web portals are communication tools that help businesses connect with their clients better. They provide a single point entry for all end users and are almost always extremely difficult to integrate into existing workflow.

Cloud computing is a form of grid computing with no singular server but a multitude of servers that can act as one. They provide scalability, increasing server capacity as needed, which makes them a viable option for growing businesses. However, with the fast computing comes the need for form and design.

Software as a Service (SaaS) is essentially software without needing to install anything locally on your machine. But with the ease of deployment comes the need for scalable data storage and computing. SaaS also needs good workflow and a singular entry point for end users.

All of these options present good cases for use but they don't quite offer the right solution for you and your clients' confidential data. The reality is that you need to use a solution that provides you a hybrid from those technologies, not just one or the other. But now you have to consider how your solution adheres to current compliance levels, security, and technology choices.

When talking about data compliance, you must review your requirements for SOX, HIPAA, EUDPD, PCIDSS, GLBA, and state requirements, such as, California SB 1386. With these requirements, a breach can be devastating. A data breach is any instance where an incident happens to make personal information viewable to a source, which should not be able to see it. Ensuring your compliance is imperative to your business and should not be ignored.

While compliance is important, it is equally important to consider the security being implemented in your solution. Physical security must be in place, such as, access to the building, rooms, and servers. Independent security audits must be performed routinely. Environment elements must be considered, such as, power, heating, and cooling. Equipment, like redundant hardware and fail-over internet connections, are a must. Network security and account security are essential for secure transactions to occur, so ensuring that SSL, network technicians, sessions, and caching, are all in place, help create a more solid solution. Security is a much larger issue than what bit-strength the SSL certificate is; examine all aspects of security before making a choice.

All of these options are enough to make your head hurt for days and give you panic attacks. But finding a solution can be a lot easier than you think. Make sure your solution allows for these features: integration into your existing workflow, scalability, singular entry point for your clients, the ability to store, transfer, gather data securely and quickly, and is a simple solution to your complex needs.

When considering confidential data, you must examine the life cycle of the data; every type of confidential data will be created, stored, transferred, and, at some point, destroyed. You must decide which of the previous choices you want in your solution; this will affect your choice of options and cost. Data rights are also often overlooked when choosing an option; you should examine: if your client needs access to data from multiple companies, your client needs their employees to have

access to just their company, your client needs to have their vendors (i.e. bank) to have access to their data, or if the bank needs information from multiple clients of yours. Again, these choices will affect the cost of your solution.

Many solutions you'll find on the market today will coax you in with fancy but rather useless features while completely ignoring the ability to track historical data. Tracking confidential data history is very important; every solution choice should be able to track creation, changes, reviews, and delivery. If your solution doesn't allow you to track the history of your data, you can be sure that you are putting your practice at risk.

Your confidential data solution should offer you the ability to control the confidential data whether it is sent to your client, from your client, and or when you are no longer retaining a client.

Overall, the best solution should always be a hybrid of confidential data and web portals. Your solution should not force you to change your workflow; it should, however, always keep or improve security, provide easy end user involvement, and be very simple to manage. Choosing a confidential data and web portal solution doesn't have to give you chest pains.

*Randy Johnston is a nationally recognized educator, consultant, and writer with over 30 years experience in Strategic Technology Planning, Systems and Network Integration, Accounting Software Selection, Business Development and Management, Disaster Recovery and Contingency Planning, and Process Engineering.*