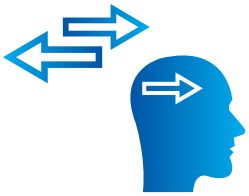
THE FUTURE OF BANKING



Do You Know Where Your Data Is Stored?

"Our methods simplify your risk assessments, policies and procedures. We eliminate the time consuming, tedious and costly process of mapping the various data elements."

— MARK C. DITTMAN, IBT CEO

With all of the storage options today, it is difficult to know where your Non Public Information (NPI) is stored. With the cloud, virtualization, and traditional media as options, sometimes you have to work to find what you are looking for. Adding to this complexity, regulatory compliance is asking that you move beyond knowing that your NPI data is stored with your processor, but now expects you to know where the data is stored – down to the physical location of the data.

As virtually everything in the business moves to imaging, the volume of data needing to be managed for general access, disaster recovery and business continuity is daunting. Coupled with the requirement to document where our data is stored, who has access, and what systems have access, meeting this compliance requirement may test the ability of many practitioners.

At IBT, all NPI image data is managed in a single storage silo and encrypted, not only when accessing the information, but also while it sits idle on the storage servers. IBT's approach to data management goes a long way toward assisting you with compliance and process management, which in turn helps you manage overall risk, and provides better management of your NPI, business continuity and disaster recovery preparedness. IBT knows that NPI compliance is part of overall vendor management. Our methods simplify your risk assessments, policies and procedures. We eliminate the time consuming, tedious, and costly process of mapping the various data elements.

Compliance around data storage has become a focus point during internal and external audits. Simply knowing what vendor is storing your data is not sufficient. Mapping where all of your data is maintained is not just as simple process of drawing a map of the locations, but is part of your overall policies and risk assessments. It, like all compliance, is ever-changing and you must build in the monitoring and movement of this information as part of your daily processes.

When you know where your NPI data is, you will need to identify those outside of traditional NPI or Core Storage vendors. You should understand how they manage or maintain the data once it is accessed. For example, an online banking system will access core data for balances and transactions. It may also access check and statement images for viewing and downloading. You will need to determine the length of time the data is maintained, and whether this data is encrypted.

If you are using a third party service provider, it may mean your data is stored in multiple physical locations and countries, especially if they are a cloud-based application provider. Microsoft states that it maintains between 10 and 100 data centers. If you input data from North America, the data may be stored in three named cites, but also in other US locations. This may expand your compliance scope and effort.

IBT®

1101 Arrow Point Dr. #305, Cedar Park, TX 78613
512.616.100 | sales@IBTapps.com | IBTapps.com