

How Automating the Financial Close Helps Healthcare's Office of Finance Drive Savings and Security



KEY CHALLENGES:

- A spreadsheet-based, manual process filled with billing mishaps and multiple areas of inefficiency slows down reconciliation efforts
- Exposure to significant financial risk due to unreliable internal controls
- Staff and budget shortages mean more work with less resources
- Securely protecting PHI in compliance with HIPAA and reliably safeguarding against cyberattacks

OUR RESEARCH:

To ensure financial stability, a healthcare facility's office of finance must implement an efficient and effective Record to Report (R2R) process, all while securely protecting and handling PHI.

Maintaining a manual process dependent on spreadsheets, binders and emails makes these goals unachievable, as the data can easily be inputted incorrectly or shared with people who should not have access.

Copyright © 2018 Trintech, Inc. All rights reserved

PROBLEM AREAS:

- Operational Inefficiencies
- Lack of Visibility
- PHI Security Risk

As the industry grows,
30%
of back end billing revenue comes directly from patients
Healthcare Finance

Only
34%
of providers have a cybersecurity audit process
PwC Health Research Inst.

Despite changing payment method trends, only
48%
of healthcare business have adopted new technology
HFS Research

PHI is
50^x
more valuable on the black market than financial info
HIT Consultant

REVIEW YOUR CASE HISTORY

While credit cards are easily canceled when lost or stolen, medical records can be compromised for years.

However, the majority of healthcare providers still rely on manual processes, such as spreadsheets, for reconciliation and patient record storage, despite a considerable increase in the number of transactions.

As the healthcare industry continues to grow, healthcare providers must be prepared to handle processes as efficiently and securely as possible as they face increased scrutiny and the need for transparency throughout every step of the financial close process.

Now, it's time to review your own R2R case history to make sure you aren't leaving your organization vulnerable by skipping the necessary precautions that help it remain immune to infection.

Copyright © 2018 Trintech, Inc. All rights reserved

REVIEW YOUR CASE HISTORY

The reluctance to change and fear of an imminent cyberattack both come from a reliance on outdated methods and technology.

However, this dependence on outdated, manual methods to perform easily automated tasks adds unnecessary burden to already thinly-stretched F&A teams.

For more information on why manual methods are unacceptable, read the eBook

[READ MORE](#)

There has been a **Fifty-Five Percent** increase in the volume of manual transactions because of online portal use.

Healthcare Finance

Ninety-Five Percent of hospitals with 200+ beds worry about cyberattacks. (*Black Book Survey*) However, despite the majority of cyberattacks targeting on-premise infrastructures, many hospitals continue to host their software solutions on-premise instead of in the Cloud.

\$10 Million

Ten million dollars in accounting errors have been reported in annual audits from hospitals with no internal audit controls.

USA Today

For more information on our HIPAA compliance, visit our website

[LEARN MORE](#)

Copyright © 2018 Trintech, Inc. All rights reserved

FIND A CURE



By automating the reconciliation process with a cloud-based, RPA-driven solution, the US healthcare industry would see significant cost savings.



The "infection" of overloaded manual processes has afflicted the office of finance for long enough, but advantages in technology, such as RPA, can cure several types of R2R ailments. Overall, robotic process automation (RPA) and the use of software robotics emulates the tasks business operations individuals typically conduct via automated solutions.



What's more, Risk Intelligent RPA creates a reliable risk-mitigation framework to allow your organization to thrive in today's risk-based world.



[OUR PRESCRIPTION FOR AUTOMATION](#)

\$11.1 Billion

Automation could save the healthcare industry up to \$11.1 billion annually.

CAQH Index

Copyright © 2018 Trintech, Inc. All rights reserved

"Health systems can use RPA to more easily determine what a patient's potential financial responsibility would be, eliminating a lot of that manual effort and getting data directly from payer websites automatically."

Senior Regional Director, Recondo Technology

Source: Becker - 2018 Hospital CFO Report

HIPAA

To keep all data secure while in transition and at rest, as required by HIPAA, Trintech has put in place specific cloud-security measures including, but not limited to:

- Well-configured, state-of-the-art load balancers
- Encryption capabilities
- Web application firewalls to protect from:
 - Denial of Service attacks
 - SQL Injections
 - Cross-Site Scripting
 - The most common types of hacking attacks
- More up-to-date patches than the average enterprise-size company



Trintech's Cloud Security team provides support and expertise that will help your team stay focused on mission-critical activities instead of the maintenance of your vendor-provided software.

[READ THE CLOUD BROCHURE](#)

MAKE A FULL RECOVERY

With complete automation of the reconciliation process within R2R, patient billing transactions will be matched and closed more efficiently, capturing more provider revenue, clearly identifying missing payments and ultimately allowing the office of finance to enable best-in-class patient care through responsible management of your organization's financials.

Beneath it all, patient data will be securely stored in the Cloud.

Up to
70%

reduction in data costs due to RPA implementation
Becker Hospital Review

88%

of healthcare IT organizations using cloud-based solutions saw their costs reduced by 20%.

continuum

