cadency
BY TRINTECH

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:

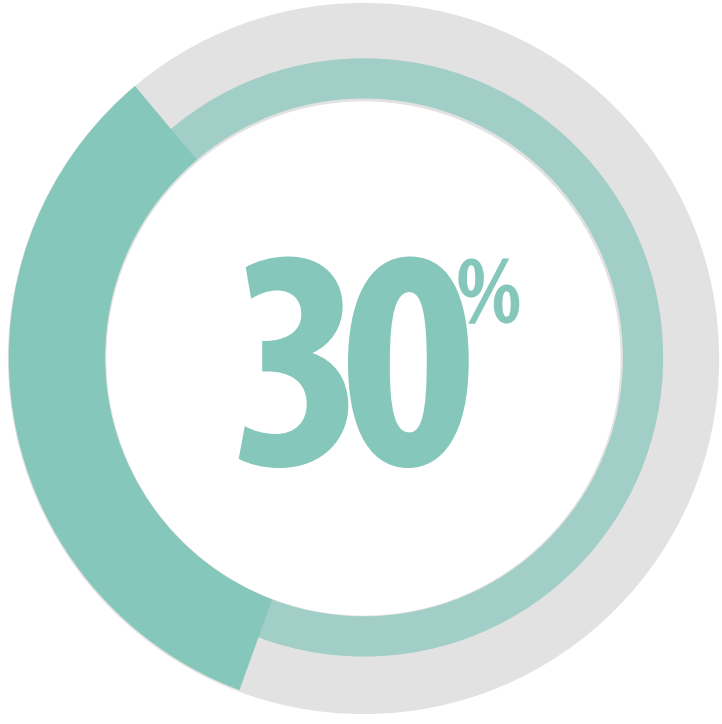
- To ensure financial stability, a healthcare facility's office of finance must implement an efficient and effective Record to Report (R2R) process, all while securely protecting and handling PHI.
- Maintaining a manual process dependent on spreadsheets, binders and emails makes these goals unachievable, as the data can easily be inputted incorrectly or shared with people who should not have access.

PROBLEM AREAS

OPERATIONAL INEFFICIENCIES

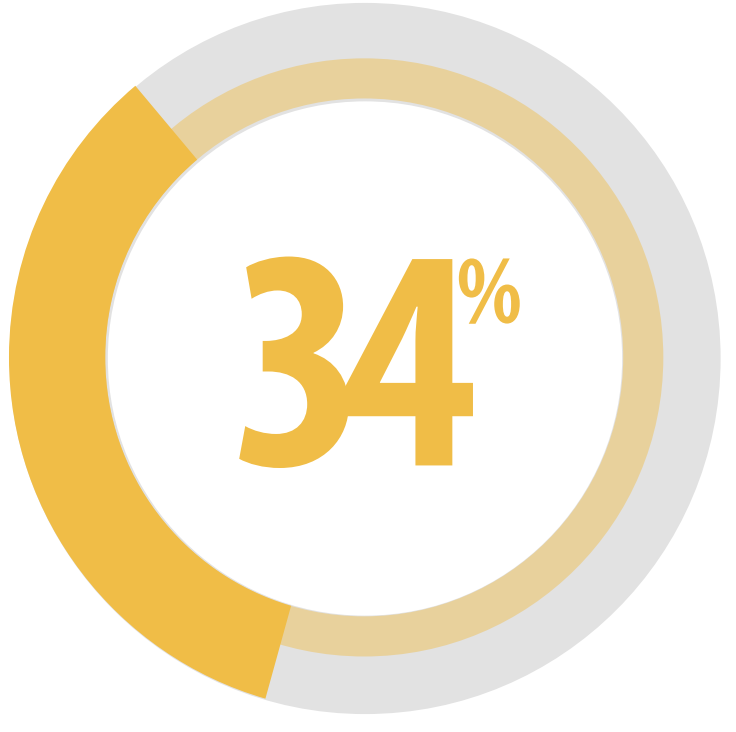
LACK OF VISIBILITY

PHI SECURITY RISK



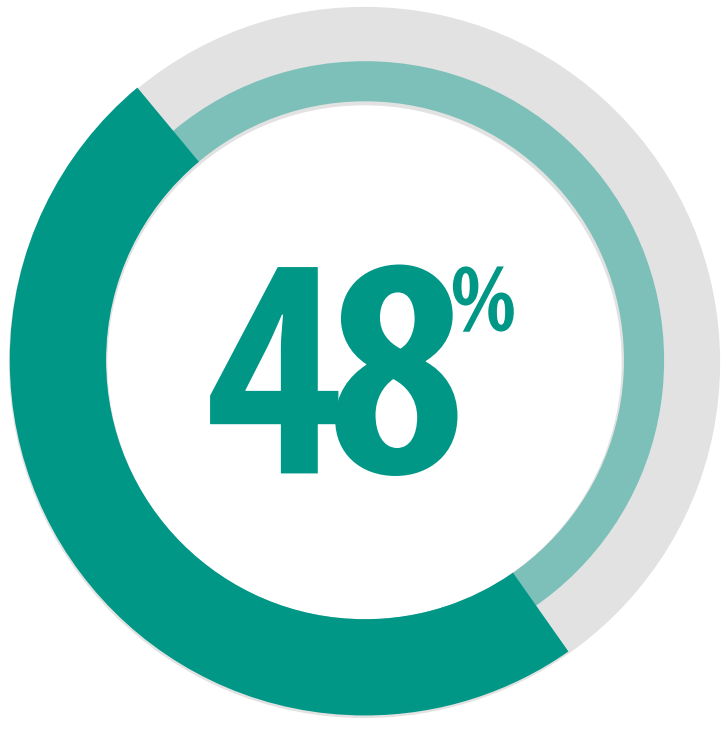
As the industry grows, 30% of back end billing revenue comes directly from patients

Healthcare Finance



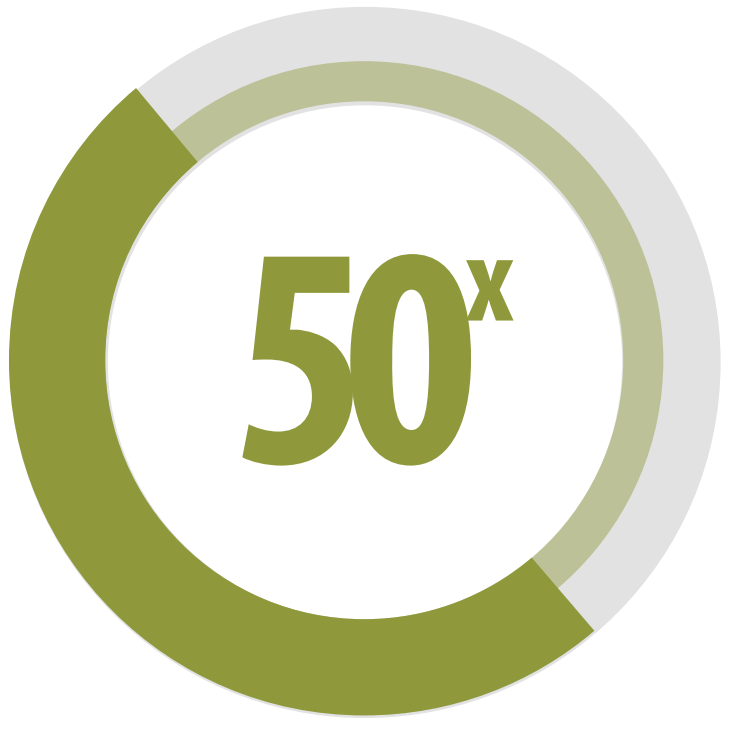
Despite changing payment method trends, only 34% of healthcare businesses have adopted new technology

HFS Research



Only 48% of providers have a cybersecurity audit process

PwC Health Research Institute



PHI is 50 times more valuable on the black market than financial info

HIT Consultant

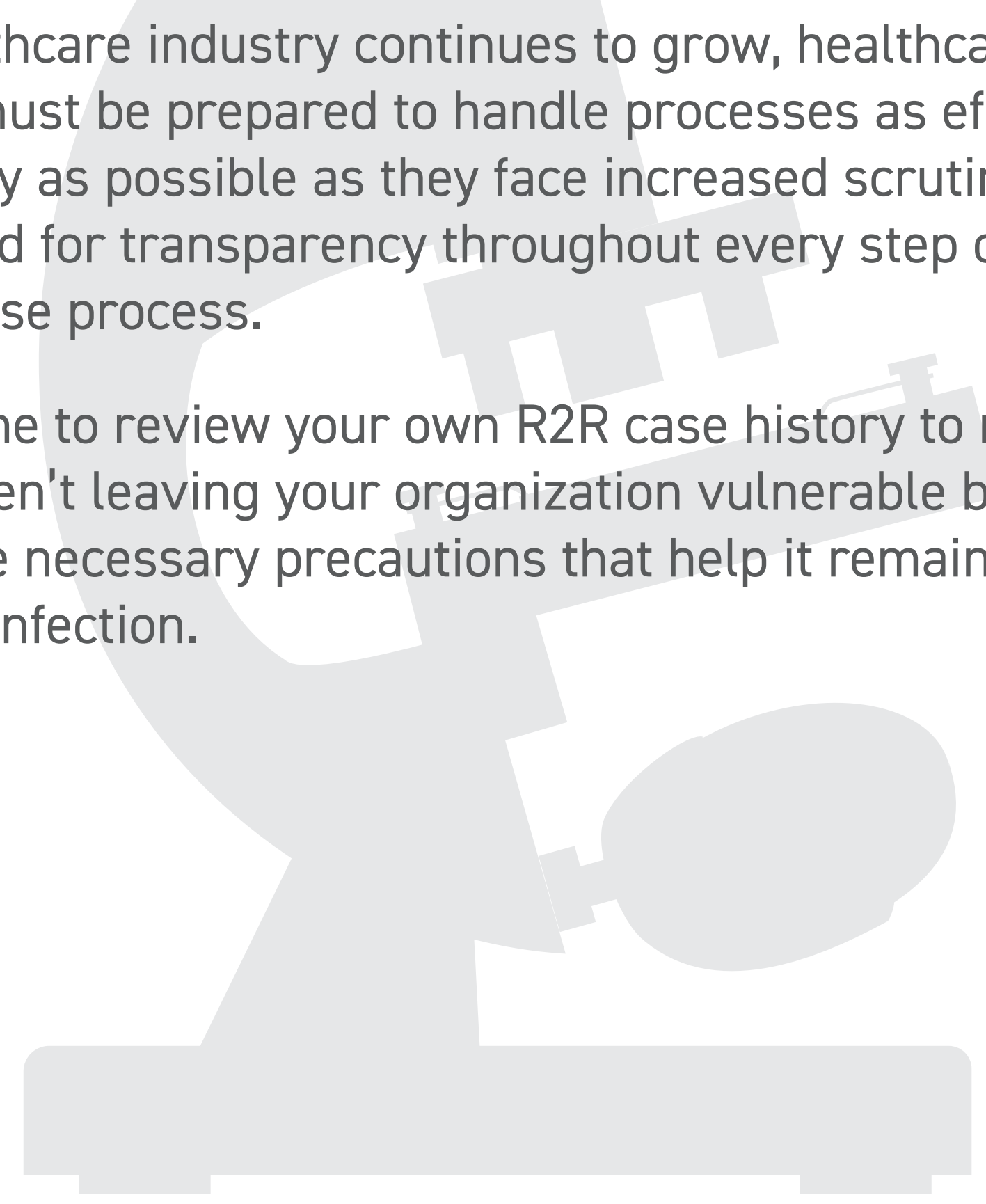
REVIEW YOUR CASE HISTORY

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.



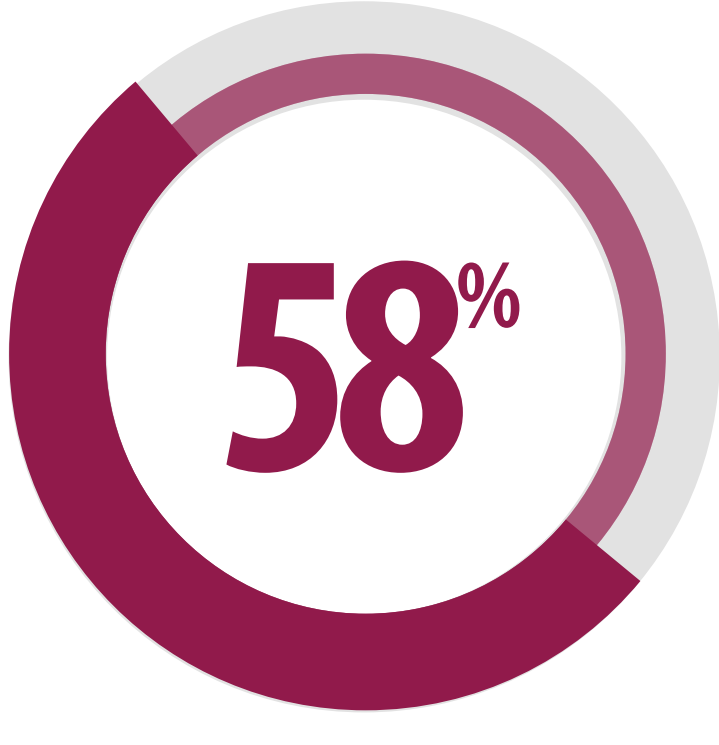
REVIEW YOUR CASE HISTORY

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.

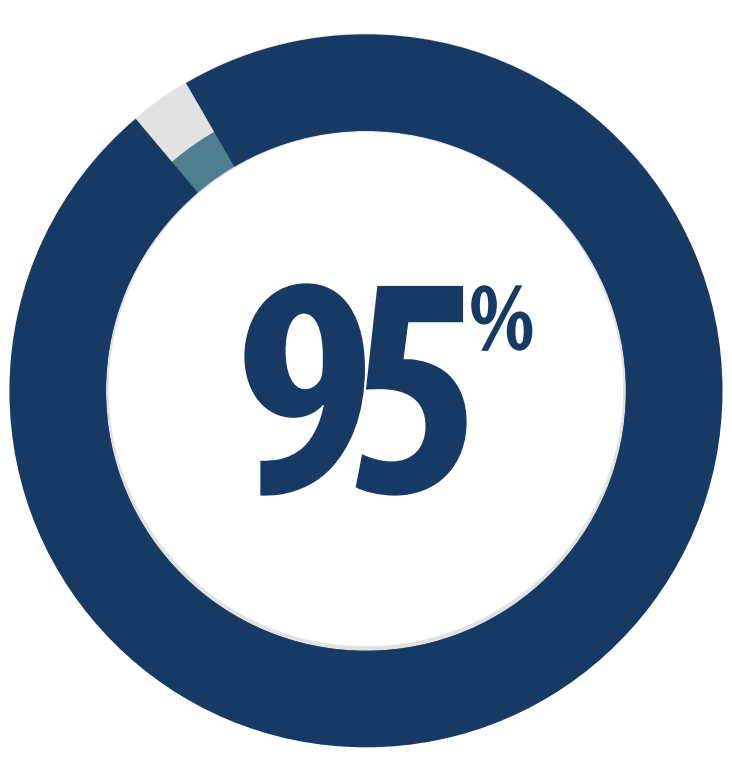
For more information on why manual methods are unacceptable, read the eBook

Learn 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

$10 Million

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.

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

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 advances 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 manual methods.

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

> "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*
- More up-to-date patches than the average enterprise-size company.

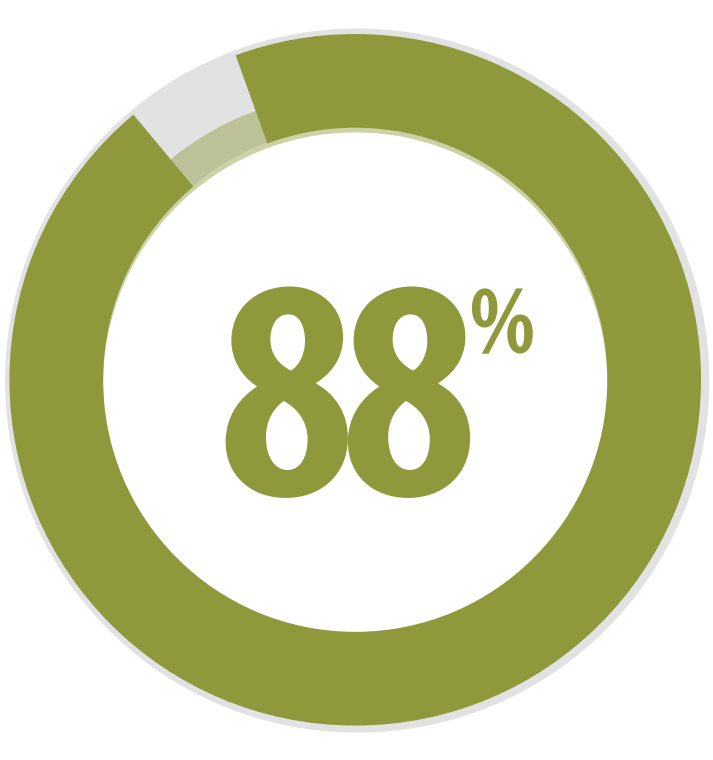
Trintech's Cloud Security team provides support and expertise that will help your team stay focused on mission-critical activities instead of the maintenance of your vendor-provided software.

Read the Cloud Brochure

HOW TO MAKE A FULL RECOVERY

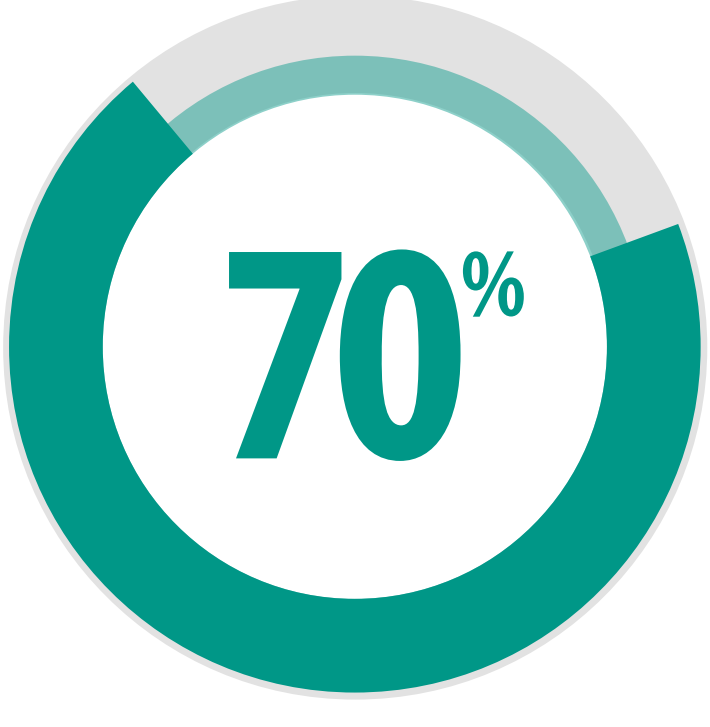
With complete automation of the reconciliation process within R2R, patient billing transactions will be matched and closed more efficiently, capturing more provider revenue, clearly identifying missing payments and ultimately allowing the office of finance to enable best-in-class patient care through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

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



Up to 88% reduction in data costs due to RPA implementation

Becker Hospital Review



70% of healthcare IT organizations using cloud-based solutions saw their costs reduced by 20%

continuum

TRINTECH.COM

cadency
BY TRINTECH

Learn More