

WHITEPAPER:

Top Four Safety and Security Trends to Watch in Healthcare in 2022

Safe Return to the Workplace

What's still top of mind for healthcare in 2022 are the continued impacts from COVID as many people return to the workplace. So for a workforce rocked, frustrated, and eventually fed-up with the pandemic, returning to work safely is foremost.

This entails significant operational challenges for healthcare providers who are under pressure to quickly recognize and adapt to priority trends. With no respite in sight, hospitals and clinics have not slowed down in fulfilling their important public health role. All the while, they are faced with mounting operational pressure from internal and external drivers that demand hospitals meet rising standards for patient safety, data integrity, security, and compliance.

2022 Trend Drivers

A safe return to work is grounded in understanding those high-impact drivers which crosscut people, workflows and technology, all in order to identify solutions that also crosscut the same areas. JADAK, a Novanta Company, has identified four trend setting drivers, and from out of those trends, presents solutions suited for healthcare providers where advanced RFID technology plays a substantial enabling role.

Driver 1: There will be more users and new role types in clinical settings, driving the need for process improvements that keep patients and staff safe.

Driver 2: There will be more connected and mobile devices overall, challenging data security efforts with a wider and more complex threat surface.

Driver 3: HIPAA compliance continues to pressure drivers 1 and 2, looming heavy financial fines and jail time for violations to ensure patient confidentiality.

Driver 4: The impetus to improve productivity and ROI will not abate.

These drivers are not new, and the effort to cope with them has been extensive. Organizations, like HIMSS (Healthcare Information and Management Systems Society), have committed to overcoming challenges in healthcare through the use of information and technology, and comprehensive efficiency models like Quadruple Aim. Quadruple Aim comprises four fundamental aims—reducing costs; improving population health, patient experience, and healthcare team well-being. Overall, the model focuses on the quality of the total healthcare experience as shared by both the patient as well as the healthcare provider.

In practice, Quadruple Aim presents quality goals for hospitals to run after, but doing so without utilizing technology and improved processes that enable staff to reach goals hampers productivity. Productivity failures are often contributed to by physician and staff burnout from inefficiently chasing quality goals.¹ But hospitals that adopt new measures, like efficient process changes, or tracking technology, have less

¹ <https://pubmed.ncbi.nlm.nih.gov/30803733/>

need to trade-off quality for productivity. The key for hospitals is to identify those key improvements that translate into significantly optimized workflows, ones which can move the needle for multiple goals.

The need to identify crosscutting solutions is well illustrated by the results produced by some simple interventions in addressing work roles and processes. In an efficiency-focused study, the results showed that the intervention team offered 48% more patient slots than the control teams, and staff were able to complete electronic health records (EHR) within their scheduled shifts (previously, EHRs piled up, and were completed after hours). Contrastingly, solutions that target only one aspect of the Quadruple Aims lead to less impressive productivity improvements. For instance, mindfulness and stress management interventions may target the healthcare team's well-being, but they do little to directly impact the other aims. What this means is that by addressing inefficiencies with key interventions, hospitals can potentially double their service capacity.

The following trends respond to the four identified drivers that lead to cross-cutting solutions which help healthcare providers address multiple quality goals while improving productivity.

Trend 1: RFID Solutions Promote Touchless Access Controls Mitigating the Risk of Spreading Infection

Trend 1 Key Take-aways

- Hospitals are adopting technologies that enable touchless processes and touchless access.
- Technologies that leverage RFID and systems integrations help hospital IT become more holistic, efficient, and capable of achieving a new business ethos, such as touchless access to patient information anywhere.

Touchless access controls help to improve the seamlessness of workflows, moreover, they effectively reduce the spread of infections especially when used in conjunction with other health protocols. For this reason, adopting touchless access control solutions is the highest priority trend in 2022.

Driving this trend is the close interaction of doctors, staff, and patients within the clinical setting. Also factored in is the size of hospital care teams. The expectation is that, for healthcare occupations over the next eight years, employee growth will reach 16%.² Yet hospital teams are more dynamic than that. From 2016-20 staff turnover in hospitals rose from 16.1% to 19.5%.³ So, healthcare providers should expect an increase of staff, but also anticipate a revolving door dynamic. It's a situation characterized by a constant stream of new and outgoing health vectors, as well as security threats. Meaning, hospital IT departments will be challenged with managing the credential lifecycles, from access provisioning through credential revocation, for a wide number of staff as they turnover.

While security is important (see trend #2), preventing the spread of infection during a time of "return to work" following a pandemic is more so, and no other solution enables the same touchless controls as RFID technology. RFID technology has versatile and flexible features to suit traditional and custom applications. RFID provides means to connect patients to their records, enabling access to patient information from any authorized access point. Underpinning workflow orchestration systems, RFID enables the means for real-time location systems (RTLS) that track patients, equipment, inventory, specimens, and pharmaceuticals. Importantly, RFID-based access controls are used in authenticating

² <https://www.bls.gov/ooh/healthcare/home.htm>

³ <https://www.statista.com/statistics/1251378/staff-turnover-rate-of-hospitals-in-the-united-states/>

staff, allowing them to quickly, and securely access hospital systems and patient information. RFID's touchless characteristics and capabilities make it a key technology in preventing the spread of germs.

Trend 2: Adoption of IAM + SSO in Healthcare to Streamline and Secure Workflows

Trend 2 Key Take-aways

- Hospitals are adopting frictionless security technologies to streamline workflows and ensure data security.
- Single Sign-On (SSO) technologies integrated with Identity and Access Management (IAM) software, and extended with RFID technologies for “touch-and-go” access, help overcome device proliferation in the face of combating the spread of infection.

Trend 2 is in response to the growing number of connected devices (smart devices, mobile devices, and point-of-care devices) relied upon in clinical settings and inundating staff. Subsequently, hospitals are making interventions to prioritize security—a survey found that 49% of executives are dropping risky BYOD policies, and adopting policies that assign rugged and durable, hospital-owned devices to healthcare staff, folding them under their IT and data security umbrella.⁴ In doing so, they reign in control of the threat surface created by the influx of new devices.

What is needed to improve healthcare quality alongside data security is frictionless security. Touchless RFID contributes greatly to frictionless security. To go frictionless, though, means that hospitals support the aim of making security both unobtrusive and comprehensive, which liberates time from the clinical workflow and improves the delivery of care. IAM (Identity and Access Management) combined with RFID and SSO (Single Sign-On) technology promotes the aims of frictionless security.

Single sign-on is a workflow efficiency and cost improvement measure that may be more impressive than its application as a security feature. One method, for example, is to assign credentials to an RFID badge, enabling “touch-and-go” access for authorized users to hospital systems at security control points or workstations. In a study of the clinical impact of SSO, both quantitative and qualitative improvements were observed. The one-week study (which did not utilize the convenience of RFID but instead a single workstation password that allowed automated signing in to further subsequent systems), showed an annualized net gain of 1461.2 hours of liberated staff time, equating to over \$92,146 of costs savings per annum.⁵ Qualitatively, there were also improvements in clinician satisfaction, reduction in staff turnover, and improvement in the timely completion of EHRs.

Furthermore, combining IAM with SSO gives hospitals a comprehensive approach to security and helps to reduce time, costs, and security overhead in dealing with two factors: the growing number of devices, and the growing number of staff using those devices. The key security approach for this situation relies on “zero trust” principles that dictate no one is trustworthy, everyone deserves to be verified, and the tenant of “least privilege” tightly wrapping user privileges to their security group. IAM software provides role-based access, usually defined by job function, and centralizes management controls that empower security teams to easily manage credentials.

Enterprise IAM software, like leading healthcare digital identity solution [Imprivata](#), provides secure role-based provisioning for hospitals, across every device, desktop, and workflow. These packages are ideal

⁴ <https://www.zebra.com/us/en/about-zebra/newsroom/press-releases/2021/seven-in-10-hospital-executives-acknowledge-need-to-invest-more-to-maximize-staff-efficiency.html>

⁵ “Clinical impact and value of workstation single sign-on” PDF

central hubs for conducting compliance, audit, and risk reporting functions, and integrating cross-cutting technologies, like JADAK's Secure Access solutions portfolio that includes the [HS-1RS Secure Hand Scanner](#), the [ThingMagic M3e Secure Access Module](#), and other custom engineered RFID technologies.

In a case of a patient receiving her prescription, a doctor can log on to the system using the HS-1RS Secure Hand Scanner touchless RFID, then accessing the patient's records via RFID wristband, and then by scanning the prescription barcodes (also touchless when the hand scanner is left in its cradle) can log the interaction. In some custom solutions, an IR scanner attached to the workstation can be set to log off the computer when users forget and leave while signed-in. This scenario illustrates a complete holistic touchless session, with minimal contact with devices and tags, and thereby substantially less possibility of spreading infection.

Trend 3: Adopting RFID Security for Patient Information Accessible Anywhere

Trend 3 Key Take-aways

- Hospitals are adopting RFID to enable access to patient data anywhere and improve patient quality of care and delivery of services.
- HIPAA impact was widened by the Omnibus Bill, and now impacts any person that comes into contact with PHI.
- Hospitals will use new technologies and education to close off weak points in handling patient information.

RFID is a powerful technology that is being used in hospitals to achieve a new ethos where patient information follows patients, no matter which department, unit, or operating room they go into. Yet, for all its benefits, RFID presents unique data privacy issues for healthcare. Life-threatening urgency plays a critical factor when considering access to patient protected health information (PHI). In a life-threatening situation, there may be no time to find the patient's proper physician and the nearest physician must act immediately. In this case, one solution is to utilize an IAM that can group like skilled roles, such as physicians, who then can access patient information in urgent cases, recognized in the moment by their RFID badge credentials.

Yet, accessing patient information with RFID technology poses challenges that are in opposition with HIPAA requirements, namely RFID is meant to be universally open and accessible, while HIPAA attempts to restrain access to such patient data, potentially stored on an RFID chip, or from patient's tracking history as they move through the hospital.

This is important, because while HIPAA legislation established the privacy rule that outlines patient information privacy, privacy issues, to clarify, differ from security concerns. Whereas data security addresses data integrity and availability, data privacy focuses on how patient confidential information is collected, used, and released (this information extends far beyond IT).

One solution to protect patient information requires integrating multiple technologies to overcome the technical of RFID openness. Software solutions can map RFID badges to a secondary ID which then is used to confirm access to patient data on a central system, rather than store that data on the card itself. In this scenario, anyone with insufficient access can read the RFID, but the patient information residing on a central system effectively remains locked away.

Another option, use [JADAK's M3e Secure Access Module](#) enabled with HID to read encrypted badges. The M3e module can be used to read securely encrypted iClass contactless badges popular in hospitals

and clinics. Moreover, this embedded module has a uniquely integrated Secure Access Module capable of access both public and encrypted RFID tag information, accessible and customizable using the established ThingMagic Mercury API. In all, the M3e is equipped to communicate securely and manage security keys.

Access to patient data anywhere can have a tremendous positive impact on the effectiveness and productivity of critical hospitals and clinics. But, HIPAA consequences applies to any organization that touches PHI. Protected health information (PHI) encompasses anything about the patient: billing records, patient information, healthcare provider data, health insurance information, and treatment and care information. This means any nurse, admin, or doctor that interacts with this PHI in their day to day are subject to HIPAA. This was widened by the 2006 Omnibus Rule, which compels “business associates” to report security incidents pertaining to breaches of PHI—business associates including even non-medical personnel, like IT staff, lawyers, accounting firms, and cloud providers, etc.

This atmosphere of data privacy further challenges hospitals who attempt providing anywhere access to patient information in order to promote improved quality of care delivery. This raises the issue, how to limit access to patient data but maximize access for as many authorized users as possible? In this light, technologies that streamline and secure potential points of attack need to be integrated to seal off those weak points. Further, education about HIPAA and the severity of violations will be a continuing effort for all staff who enters, uses, or transfers patient PHI in any way.

Trend 4: Workflow Orchestration for Optimizing Hospital Service Delivery

Trend 4 Key Take-aways

- Sophisticated hospitals are integrating automation and real-time tracking to improve their workflows and improve ROI.
- Coveted technologies will cross-cut many key goals and eliminate human errors, streamline workflows, and prevent the spread of infection.

Ambitious hospitals have adopted workflow orchestration for efficiency gains and ultimately very attractive ROI. Orchestration applies automation to the tracking of staff, patients, inventory, equipment, and events, essentially integrating into real-time tracking systems (RTLS) and making sure that the whole hospital is running smoothly. RTLS can also help verify if safe-distance protocols are being followed, and that hospitals don't become dangerously crowded.

More so, these systems are exceptional in their custom capabilities. While patients can easily be tracked via RFID wristband, the same information can be piped to many other systems. Staff can be notified about upcoming events on their mobile devices. Surgical inventory can be requested electronically, even confirmed available in the operating room before upcoming operations. After, following operations, housekeeping can be notified that operating rooms are available and need to be cleaned and sanitized.

Workflow orchestration has the potential of improving workflow efficiency in astounding ways. This trend simply states that hospitals are adopting ways to eliminate human steps that can contribute to errors, like taking inventory, and thereby reclaim time for staff to supply the best patient care.

Enabling Secure Access with Advanced, Integrated RFID Technology

What the trends together are saying is that technologies that are secure, enable seamless and touchless access, and easily integrate into established hospital and laboratory systems prove to be coveted solutions in the effort to keep workforces safe as they return to work. JADAK's family of secure access products are ideal for leveraging the touchless properties enabled by RFID to reduce the footprint of medical devices, enabling real-time inventory tracking, and providing a means to further secure and protect patient information in hospitals, labs, and clinics, and overall prevent the spread of infection.

For OEMs, a partnership with JADAK provides custom engineer-to-engineer expertise in designing and implementing versatile and customizable secure access to RFID communications. Additionally, JADAK solutions integrate with leading tech partners Imprivata and HID, supporting holistic IAM and touch-and-go security.

JADAK's has two state-of-the-art healthcare solutions to help hospitals achieve their touchless safety and security aims.

The [FlexPoint HS-1RS Secure Access Handheld Barcode Scanner](#) is a single small footprint device, designed specifically for the particular needs of healthcare applications, encased in a sealed IP54 medical grade, durable against sterilization and disinfectants. The Flexpoint, as the name implies, is a single flexible access point, capable of reading over thirty-two HF/LF RFID protocols, scanning fourteen 1D/2D protocols, and integrating into any OS and workstation.

[Witness how healthcare workflows are immediately simplified using the FlexPoint HS-1RS Secure Access Handheld Barcode Scanner in this video demonstration.](#)

For embedded RFID designs, the [ThingMagic® M3e HF/LF RFID Secure Module](#) developed in partnership with HID Global, provides a platform and API set for maximum customization of OEM solutions, with a wide array of RFID protocols, including HID Seos, HID iCLASS as well as NXP and EM-Micro tags. The M3e is the only LF/HF module in market with a completely integrated Secure Access Module (SAM) that specifically secures communications to RFID tags. These capabilities makes the M3e Secure Module ideal for seamless, safe, and secure access for healthcare applications.

About JADAK

JADAK, a business unit of Novanta, is a market leader in machine vision, RFID, barcode, printing, and color and light measurement products and services for original equipment manufacturers. The business designs and manufactures custom embedded detection and analysis solutions that help customers solve unique inspection, tracking, scanning and documenting challenges. JADAK is based in Syracuse, New York, with sales and technical locations across the globe. For more information, visit www.jadaktech.com.