consensus Cloud Solutions

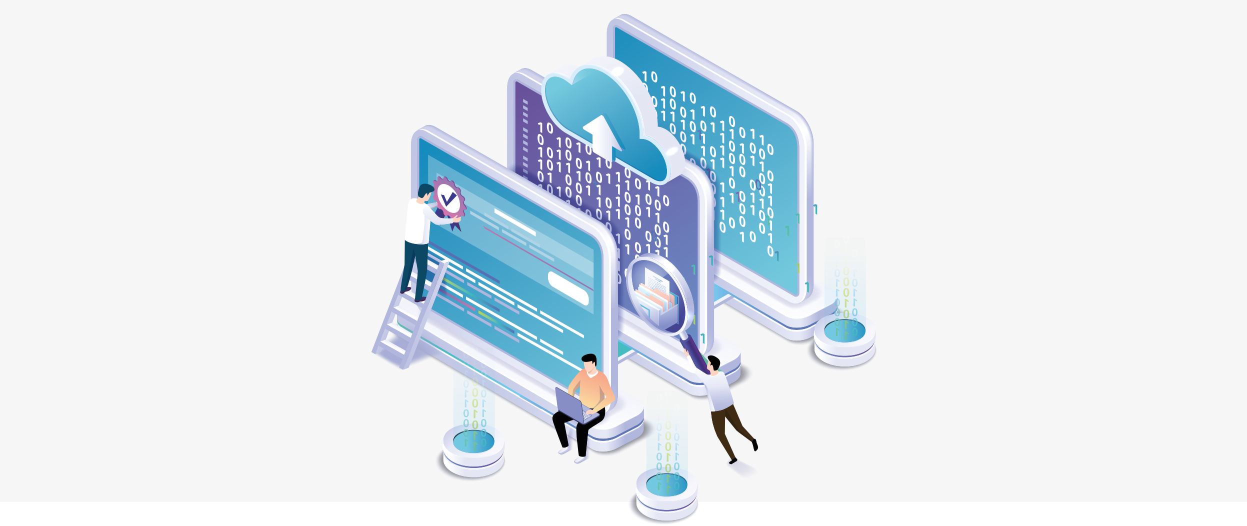
Planning for Hospital Systems' Downtime

Ensuring that Patient Care Continuity is Uninterrupted When Systems Go Offline

'Always on' hospital culture promotes patient safety, while meeting federal requirements.

TABLE OF CONTENTS

Plan Now for Incidents that Surely Will Occur (and you can't control)



By their very nature, hospitals are "always on." Through tornadoes and hurricanes, multi-car pileups, and other emergencies large and small, hospitals and health systems are on the front lines of healthcare, ready to triage, evaluate, and treat everyone who comes through their doors.

But what if that care comes to a sudden halt? What happens when the hospital floods or endures a storm surge? What about an extended power outage or a major cyberattack? How can a facility continue to care for patients in the middle of an organization-wide crisis?

While companies in all industries should have some sort of business continuity or disaster recovery plan, it's a critical consideration for hospitals. Because hospitals are in continuous operation, an outage of any duration can reduce the quality of patient care or force patients to go elsewhere. In addition to putting patients at risk, an unplanned outage can tarnish a facility's reputation and leave it vulnerable to potential lawsuits.

Scheduling and monitoring planned downtime for software maintenance and upgrades, facility improvements, and other activities is just as important as preparing for unexpected emergencies that can knock a hospital offline.

However, implementing a downtime solution can be challenging. Manual workflows that process and distribute physical documents are costly, unsafe and inefficient, while designing a homegrown solution can burden an IT staff with unneeded complexity.

In this white paper the following topics are addressed:

- Types of downtime and the causes
- Cybersecurity risks for hospitals
- Direct and indirect costs of downtime
- Best practices for downtime planning
- Consensus' solution for downtime - a case study

Adopting a downtime solution will help keep patient care at a high level despite circumstances out of the hospital's control, while helping hospital leaders to rest easy, knowing that facilities will continue to operate in the face of unpredictable or unforeseen circumstances.

Hospitals Must Make Provisions for Planned and Unplanned Downtime

Planned software upgrades, new installations, construction projects, and much more, can disrupt normal hospital operations, which never stop. Described in layman's terms, it can be like trying to change a car tire while the vehicle is in motion.

Careful consideration of the potential impact on all affected areas and personnel is a must, as are contingency plans, should the software implementation or project not go the way it was foreseen. What if two hours of expected downtime in the middle of the night turns into 10 hours that impacts early morning surgeries? No project should proceed without prior deliberation and due diligence to ensure that any impacts to patient care are kept to a minimum.

And then there is unplanned downtime, internal or external events that hamper a hospital's ability to deliver patient care. One often thinks of a natural disaster, a fire at the hospital, or a severe storm that impacts businesses across an area.

Power outages are also common occurrences that hospitals must plan for. Other threats might not rise to the level of planning but should be accounted for in any business continuity plan. IT software or hardware outages are possible, which can limit or prevent access to patient files. Hospitals and health systems often operate legacy software that can lose its connectivity to the wider network. Hardware servers can unexpectedly fail. Failure to keep software updated can open up computing networks to hackers.

Hospital executives and IT leaders must honestly assess the state of hospital operations and plan for the most common scenarios that can bring down IT systems and hospital infrastructure. A software solution that aggregates critical data on a schedule and distributes information to computers that are not connected to the wider network can help hospitals continue to operate in a crisis.

Cyberattacks Are an Ongoing Threat to Hospital Operations

Unfortunately, cyberattacks or ransomware attacks, pose an increasingly common threat to hospitals that must be anticipated and planned for. Bad actors can exploit software vulnerabilities or human failures to infiltrate IT networks, siphoning off patient data for nefarious purposes. They also can lock networks, crippling a hospital, while making demands for payment to return data. Even if hospitals pay a ransom, there is no guarantee the data will be returned or that hackers won't attack again.

Over the past decade, the number of breaches increased by 250%, before leveling off in 2022 at

just under 700 breaches. Good news, right? Any positive takeaway from slightly fewer breaches should be tempered by the fact that more than 51.4 million patient records were breached last year, the highest number on record outside an anomalous 2015, when just two health plan breaches affected nearly 90 million records.

The percentage of incidents attributed to hacking and malevolent IT attacks has risen sharply over the past few years. Until 2018, hacking events accounted for fewer than 50% of all breaches. However, that percentage rose to nearly 79% in 2022. The second-largest category is unauthorized access, which accounted for 16% of breaches last year.

According to a global, cross-industry survey, nearly one-half of respondents reported enduring a successful cyberattack in the previous 12 months that prevented data access. More than two-thirds say they lack confidence that protection measures can sufficiently deal with malware or ransomware attacks, and 63% are not confident their mission-critical data could be reliably recovered after an attack.

Another report shows that ransomware attacks on healthcare organizations increased 94% between 2021 and last year, with more than two-thirds of organizations reporting an attack in the previous year — double the 2021 figure. The estimated cost to remediate a healthcare data breach now tops $10 million, including detection costs, notification, remediation, lost revenue, and negative publicity. Despite the fact that the federal government declared healthcare technology as a "critical infrastructure," the healthcare industry has topped the breach list for 12 consecutive years, incurring breach costs that are double the norm for financial services.

A 2019 attack on an Alabama hospital led to what's believed to be the nation's first fatality stemming from ransomware. The attack knocked out the hospital's EHR and patient monitors, which led to insufficient monitoring of a fetus that was born unresponsive with the umbilical cord wrapped around the child's neck, a lawsuit alleges. The child was resuscitated but suffered brain damage and died nine months later.

Hospitals deal with unexpected patient cases on a daily basis, but preparations must extend to the software and systems that keep a modern hospital running.

Cost of Downtime Goes Well Beyond Revenue Loss

Downtime costs can vary widely across industries, but many studies cite an average hourly cost of between $320,000 and $540,000. Healthcare undoubtedly would be near the top of the range — not including such indirect costs as compromised patient safety, reputational risk, and reduction of trust and standing in the community.

Not only is a reliable downtime plan necessary for quality patient care, it is mandated for HIPAA and Meaningful Use. Facilities need a software solution that fully satisfies both the HIPAA Final Rule addressing system downtime and Meaningful Use Part Two Core Objective 7. It's not enough to merely tick the planning box; hospitals must ensure downtime reporting needs are met in a safe, compliant way, with secure report encryption and distribution and 100% access to patient information.

While software is important to ensure patient data is available during an outage, hospitals ignore the human element to downtime and cyber risks at their own peril. A survey from the Information Technology Industry Council shows that 50% of IT downtime can be attributed to human error. The error may stem from workers not following standard procedures or protocols.

More than 80% of breaches involve a human in some way. Examples include someone falling for a spear-phishing campaign designed to solicit credentials, clicking on a malicious link, or a simple error that leaves a security vulnerability open to bad actors.

Any downtime mitigation plan must not only include a technology element but also take into account the oversized role humans play in unplanned downtime incidents and cyberattacks.

Best Practices for Downtime Planning

Effective downtime planning requires close cooperation among hospital executives, clinical department leaders, IT staff, and frontline workers to fully understand the breadth of what a downtime plan should entail at a particular facility.

A robust software solution such as Consensus' All Access for Downtime can take the fear and confusion out of hospital downtime and business continuity planning. Facility leaders can securely distribute clinical documents and forms from any source system, empowering staff with the confidence to maintain quality patient care during a planned EHR downtime, a network downtime, or an unplanned event.

Reporting is the primary consideration of any downtime plan. Example of reports that should be pulled include:

- Medication administration record – Dose and scheduled times of medications for a patient, so nothing is missed during the downtime.
- Medication summary – Reference list of what medications a patient has been administered and medications declared upon admission.
- Lab results – Tests performed and in process, to prevent the same test from being performed again unnecessarily.
- Census – Important to know what patients are where, and this provides a worklist for a clinician or nurse to work from.
- Nursing history – Useful when beginning the diagnostic process, including any medications (prescribed, over-the-counter, recreational).
- Rounds report – Useful for providing a worklist for a physician of patients to visit during rounding.
- Dietary reports – Allergies or special diet restrictions to prevent allergic reactions and ensure special dietary directions are followed.

The best downtime plan and the most robust downtime software won't help a hospital get through a planned or unplanned network outage without constant vigilance to ensure the plan and software are understood and ready to go. Here are other factors to consider:

- Will your physical downtime clients work during a network outage? Most hospital systems have one or more physical downtime clients that receive encrypted reports on a regular basis about device availability, however, those devices may be plugged into a power outlet connected to a generator or interrruptible power supply. Check with the hospital plant operations or maintenance team leaders to ensure a device will work when it's needed most.

- Clearly mark your downtime clients. Time is of the essence when a report is needed, so clearly mark downtime clients. Ideas include a red dot or other distinctive marking on downtime machines. A keyboard of a different color also can make this distinction, as can a prominent sign. Also be sure to put a sticker over the power button, reminding everyone to not turn the machine off. Finally, educate users on the location of the nearest downtime machine, along with how to log in and retrieve patient data.
- Adopt authentication contingency plan for Active Directory (AD) scenarios. If the network/AD is down and cached AD credentials are not an option, users should be able to call a specific help desk number and/or log in with the unit supervisor. After the downtime ends, reset the emergency user passwords for the next use.
- Put your plan and your technology to the test. Much like fire drills and other emergency preparedness drills, your downtime plan and the technology should be tested periodically. A mock downtime will familiarize people with the preparedness plans and help identify gaps and deficiencies that may need attention.

Planned Downtime Checklist

Step 1	**Monitor reports (ahead of time)** Confirm reports are being generated in the expected intervals by monitoring throughout a workday. Update any timing issues, as necessary.
Step 2	**Determine timing of reports** Compare the start of the downtime with the last expected report run, adjusting run time, if needed, to ensure complete data is available beforehand.
Step 3	**Check schedule for errors (week before scheduled downtime)** Does the scheduler application show any errors? If yes, investigate and resolve the errors. Most common errors stem from workstations that are unavailable. Compile a list of those workstations and investigate why they are unavailable. The most common reason is users have turned them off.
Step 4	**Confirm Active Directory users (week before scheduled downtime)** Check Active Directory groups to confirm all necessary users are listed (new hires, transfers, etc.).
Step 5	**Disable purge settings (at the time of the downtime)** Do not generate new reports during a scheduled downtime. Disable purge tasks prior to the downtime.

Business Continuity Case Study

FHN Memorial Hospital is the centerpiece of the FHN health system, which serves more than a half-million patients annually at the hospital in Freeport, Illinois, and at 18 locations in five counties across northwest Illinois.

When the hospital was upgrading to the MEDITECH 6.15 platform, staff realized they needed a more robust downtime solution to protect patient data and confidentiality throughout the organization and ensure that patient information would be readily available should a planned or unplanned downtime event occur. The hospital was using a homegrown solution that no longer fit their needs.

Following a demonstration of Consensus' All Access for Downtime solution, the staff was convinced the technology could cover all aspects of the organization, regardless of planned or unplanned downtime, with a robust, secure, easy to use, and streamlined solution.

The Consensus platform is separate from MEDITECH and its network, with pertinent patient data stored in dedicated downtime machines strategically located throughout the hospital. This redundant technology ensures that patient data is available 24/7 and is easily accessible to clinical staff members in the event of a downtime event. FHN also chose Consensus' project management services that included installation and configuration, automation for five reports, product training, and a knowledge transfer after implementation.

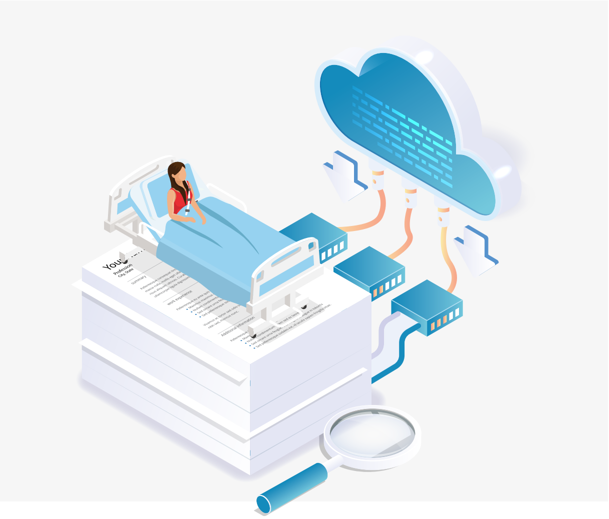
The benefits of the Consensus All Access for Downtime solution include:

- 24/7 access to data that's synchronized to dedicated workstations throughout the facility for use during scheduled or unscheduled network downtime.
- Automatically encrypted data to HIPAA standards that can be easily monitored, including as an additional backup for data access and cyber security protection.
- Cost savings due to the elimination of legacy system maintenance.
- Protection from cyberattacks and costly potential litigation that could otherwise occur due to lack of care continuity during downtime.

At FHN Memorial Hospital, five critical patient reports are run daily on a pre-determined schedule, then encrypted and distributed to the downtime workstations. Staff members from 18 departments can access reports specific to 10 active directory authentications, with more than 100 users. Departments include Cardiac Services, Pharmacy, ED, Telemetry, Ambulatory Clinics, OB, ICU, Lab, and the Cancer Center.

Benefits include:

- 24/7/365 access to critical patient data
- Uninterrupted patient care
- Less stress among staff
- Protection against planned or unplanned downtime



Conclusion

A downtime plan supported by appropriate software is not just needed to maintain patient care, but is also mandated for HIPAA and Meaningful Use statutes. Consensus All Access for Downtime fully satisfies both the HIPAA Final Rule addressing system downtime and Meaningful Use Part Two Core Objective 7. With secure report encryption and distribution; and 100%, around-the-clock access to patient information, hospitals can rest easy, knowing their downtime reporting needs are met in a safe, compliant fashion, and that patient care will not be interrupted.

About All Access

The Consensus All Access platform is the one-stop-shop for strategically managing patient data availability throughout the healthcare enterprise. All Access provides secure data availability, 24x7, throughout your organization. Much more than just a business continuity solution, this powerful web platform offers additional functionality for those hospitals looking to take their integration capabilities a step further. All Access can be extended past the four walls of your hospital to your entire healthcare community. The robust solution offers fully audited access to patient data for care providers, further improving patient safety and care transitions through proactive outreach. Consensus' components of the platform include:

- Signal - ADT event notifications
- All Access Community - access to corresponding critical patient data
- All Access Downtime - Distribution of electronic patient data in the event of network or EHR downtime

About Consensus Cloud Solutions

Consensus Cloud Solutions, Inc. (NASDAQ: CCSI) is the worlds largest digital fax provider and a trusted global resource for the transformation, enhancement and secure exchange of digital information.
We leverage our 25-year history of success by providing advanced solutions for regulated industries such as healthcare, finance, insurance, real estate, and manufacturing, as well as state and federal government. Our solutions consist of: cloud faxing, digital signature, robotic process automation, interoperability and workflow enhancement; and intelligent data extraction using natural language processing and artificial intelligence.
Our IT solutions can be combined with best-in-class managed services for optimal results. For more information about Consensus, visit **consensus.com** and follow **@ConsensusCS** on Twitter to learn more.