THE HEALING PROCESS:

How automation can help the healthcare industry improve compliance

WHITEPAPER

Executive summary

Rapid advances in technology over the past ten years have provided the healthcare industry with exceptional tools for transforming the way patients are treated. Hospitals can now collect more data than ever before, and this can be used to provide patients with more streamlined and effective care. It is an exciting time to reimagine healthcare provision: Internet of Things devices have the potential to provide real time health data to patients and doctors alike, and online video conferencing tools now allow individuals to consult a medical professional from the comfort of their own homes.

While these advances are exciting, there is also greater need than ever to ensure the vast amounts of information generated are kept secure, organized and accessible by only authorized individuals. To ensure this happens, a raft of regulations have been introduced in recent years—such as the HITECH and HIPAA acts in the United States, or Australia's Regulation of Health Information Privacy. Non-compliance with these laws can result in major fines and a loss in trust on the part of patients.

This whitepaper takes the position that complying with these regulations requires healthcare organizations to focus on the processes underlying compliance. For instance, being able to present auditors with a transparent view of how an individual patient's information has been managed will be much easier if a regular, repeatable and rigorous process has been followed each time.

Fundamentally, this whitepaper argues that automating the workflows that underlie healthcare activities will ensure that compliance requirements can consistently be conformed to.

The breakpoints
in healthcare information compliance

Besides famously swearing to "first, do no harm", medical graduates taking the Hippocratic Oath[1] also promise that:

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men…I will keep to myself, holding such things shameful to be spoken about".

Since time immemorial, privacy has been fundamental to the doctor-patient relationship. This sense of trust has been a guiding principal in the medical profession, yet in the modern era—where information is incredibly easy to access, share, copy, distribute and publish online in seconds—the need to keep private medical data safe and secure is more pressing than ever.

As helpful as it is for doctors to be able to access a patient's entire medical history in a couple of keystrokes, it also places that patient's most private, personal and often painful experiences in tantalizingly close access to hackers or individuals with malicious intentions. In most countries, a raft of rules and regulations have been introduced over time to cope with this proliferation of data and the risks associated with its collection. The laws attempt to govern this information and ensure medical practitioners keep this data safe are broad and wide ranging. However, as positive as their intentions are, they can also be confusing and disorientating.

One survey, reported in HIPAA Journal[2], found that two thirds of healthcare professionals lack confidence in the best way to share data.

Doctors and other medical professionals are often overwhelmed by the sheer diversity of healthcare regulations that affect what they can do with patient data, and how they can use it. It can be unclear how they're meant to deal with it, and many simply don't have the time to ensure they complete all data protection processes to the letter.

This whitepaper will argue that most 'break points', where data might be managed incorrectly and lead to unintended breaches, leaks or sharing of private information, arise from a failure to follow processes correctly. The whitepaper argues that it therefore makes sense to automate these processes, to ensure that they are always followed correctly and to the full, while also ensuring that the organization remains compliant and auditable.

[1] The John Hopkins University Library. 2017. The Hippocratic Oath: Text, Translation, and Interpretation, by Ludwig Edelstein. Available online: http://guides.library.jhu.edu/c.php?g=202502&p=1335752

[2] HIPAA Journal. 2015. The thirds of healthcare organizations lack confidence in data sharing. Available online: http://www.hipaajournal.com/two-thirds-of-healthcare-organizations-lack-confidence-in-data-sharing-8213/

THREE COMMON BREAK POINTS IN HEALTHCARE COMPLIANCE

Compliance with data protection regulation is fundamentally about following correct processes related to data protection and doing so consistently.

On paper, compliance seems straightforward. In practice, it can be very challenging to follow the rules to the letter. In most organizations, processes are still very often completed 'manually'. For instance, a patient referral from a general physician to a specialist will require sharing notes. This may be done by downloading a document, printing it out and posting it. Even in a more digital environment, this might involve sending email attachments containing sensitive data. This tendency to do things manually leads to inevitable break points:

1. SHARING INFORMATION

Doctors and other medical professionals often need to share data regarding a patient with one another. This might be shared via email or using a cloud-based document environment such as Dropbox. The break points here are obvious: information can become duplicated, emails can be forwarded accidentally and the wrong people might get access to the Dropbox site a few months down the line and discover private patient data.

2. CONTACTING PATIENTS

Institutions may use various methods to contact patients—from emails to text messages containing test results or letters. These methods can all potentially break down when done manually. Letters can be sent to the wrong address, emails can be sent to the wrong person who has the same name, text messages sent to the wrong phone number, etc.

3. MULTIPLE SYSTEMS

Patient information is often stored in multiple different systems, meaning individual medical staff often struggle to join the dots between data. From emails, to paper files held in different departments, servers and utilization of non-authorized data storage systems, pulling together a complete view of a patient, and also providing auditors with a total understanding of activity can be surprisingly hard.

What happens
when processes collapse?

Last summer, Illinois-based Advocate Health Care Network, agreed to pay a $5.5 million fine to the US Health and Human Services Department, the largest penalty of its kind ever in the United States . The fines were related to a string of errors at the practice, which compromised patient names, addresses, birth dates, credit card numbers, demographic data and clinical information:

- First, four desktop computers were stolen, containing records of nearly four million patients
- Second, an unauthorized individual gained access to the network of a company that provides billing services to Advocate Health Care Network and was then able to compromise about 2,000 patient records
- An employee's unencrypted laptop, containing the patient records of over 2,200 patients was stolen from a car

What does this example tell us about the importance of process when it comes to protecting patient information?

Put simply, when correct processes have been put in place, breaches are much less likely to happen:

- Of course, the major issue here was a basic security issue: information on the stolen machines should have been stored behind encrypted systems, with multiple levels of protection, meaning that even if someone could access the machines, the information would still be protected behind passwords
- However, processes would have kept the data more secure: the process of sharing of information between the healthcare provider and its suppliers should have been better managed
- Efficient processes would also have ensured that no employee would need to have downloaded so many files to their laptop, and internal audits could have been designed to alert administrators of this risky behavior

To avoid this kind of fine, healthcare organizations need to rethink their processes, and explore new approaches to managing patient data.

[3] Mangan, Dan. 2016. Huge data breach at health system leads to biggest ever settlement.
Available online: http://www.cnbc.com/2016/08/04/huge-data-breach-at-health-system-leads-to-biggest-ever-settlement.html

What is workflow automation?

Workflow automation aims to boost the efficiency of organizational processes by automating repetitive tasks and removing the potential for human error within these processes. Traditionally, such processes can easily break down for all manner of reasons—from a doctor forgetting to share the correct patient information with a colleague to a patient losing a hand-written drugs prescription and not being able to get the medicine they need.

Workflow automation minimizes these risks by codifying these processes into automated systems which significantly increase the chances of tasks being done correctly and on time. Rather than depending on oral requests, paper-based notes or emails that may never be checked or responded to, workflow automation keeps pushing these processes so they get completed correctly.

3 Healthcare processes that could be automated to improve compliance

We are living in an exciting era for healthcare, where technology offer a new vision for what healthcare means in patients' lives. At this juncture, it is highly important to take a long-term view and consider how the use of new technologies will interact with the realities of running a medical institution and, importantly, how they can be deployed in a way that ensures that institutional practices remain compliant.

Workflow automation works as the oil between these competing concerns, allowing organizations to adapt, while also helping them to follow the rules. Let's explore three key processes that can be automated to ensure your organization remains compliant.

AUTOMATING VERBAL ORDER AUTHENTICATION (VOA)

While medical professionals are increasingly asked to reduce their usage of verbal orders, high pressure situations may mean there is no choice in certain circumstances. VOAs need to be transcribed as soon as possible into a patient's medical file.

A workflow which uses a customized form, can ensure that this data is entered into the correct records immediately, with fields for:

- Patient name
- Age and weight
- Drug name
- Dosage form
- Exact strength
- Quantity and duration
- Other instructions

1. Being able to audit the status of your security controls

Internal audits are a crucial way of ensuring patient information is not being misused or abused. Auditors will want to monitor any unusual activity on your systems, such as:

- An employee viewing the records of someone who appears to be a family member
- Patient files that have not had any activity on them for a long time being opened for no obvious reason
- The files of VIPs (celebrities, politicians etc.)
- Records of patients that the employee was not involved in treating
- Records pertaining to employees who have left the organization

Unfortunately, due to a lack of resources, this kind of internal auditing often only happens when administrators suspect that some kind of misdemeanor has occurred, meaning that much of the time, there is relatively limited control. Let's see how an automated workflow might be much more effective as a means of carrying out regular internal auditing.

AUTOMATED INTERNAL AUDITING

- You set a series of rules that monitor for any kind of suspicious activity
- When an employee begins carrying out unusual behavior on the system—say, a pediatric nurse looking at the drug and alcohol records of an adult patient—a workflow can be triggered
- This could be designed to alert, via email, your head of operations
- This person could then monitor what that nurse viewed and then decide if there is anything suspicious about the behavior. If everything seems 'above board' they can simply cancel the process
- Alternatively, if the behavior does seem out of line, the workflow might provide them with a series of options: cancel that nurse's permission to view the files, send them an email asking to explain why they viewed the record, or even send an email to their manager

By constantly monitoring any unusual behavior, rather than leaving it until someone notices something suspicious, healthcare organizations can stay ahead of any potential rule-breaking.

2. Providing full records to patients

In the United States, the HITECH Act requires providers who have implemented an electronic health records system to give patients the right to obtain all their personal health information in electronic format[4]. The problem for many healthcare providers is that information is often stored in a wide range of document libraries, inboxes and cloud servers. This makes it much harder to collate the information, making institutions liable to a fine for non-compliance if they fail to send all information to the patient.

Once again, automation can help significantly here.

AUTOMATED TRANSPARENCY

- A patient decides they want to see all the records and information your organization holds on them
- By using a workflow automation tool like Nintex, they can simply enter their details into a request form on your website
- This would then trigger a workflow that searches for information pertaining to that individual across millions of lines of data in your systems
- It could also be designed to ask physicians and nurses who have treated that patient to search through their email inboxes for any information
- And it could also be designed to search through cloud-based platforms
- This could then be compiled into an automatically generated document that is delivered to the patient
- Throughout, an employee could also be charged with reviewing whether the information being included in the document is correct and pertains to the patient in question

[4] The HIPAA Survival Guide. 2017. HITECH Act Summary. Available online: http://www.hipaasurvivalguide.com/hitech-act-summary.php

3. Announce breaches

In many countries, healthcare and data protection legislation requires healthcare organizations to report any suspected breaches to patients, government agencies and even media organizations within a short time frame. When done manually, this kind of announcement faces many potential break points which can provide further damage to the organization's reputation and make penalties more painful if a 'cover up' is discovered.

Automating the process can help significantly here.

TRANSPARENCY FIRST

- A former contractor decides to steal and sell patient data online
- As soon as your organization discovers the breach, you can launch an automated workflow which will provide you with necessary deliverables: a personalized letter to patients describing the situation, an explanatory email sent to the correct government agency and a press release to go to select news organizations
- The workflow can gather all information from your systems, and also email key organizational employees asking for a statement to include in your template
- This can create a secure and sensible series of templates holding all information which needs to be released to the right people. This ensures that no further mistakes are made, and that all the correct and legally required information is sent out at the right time, even when staff may be feeling overwhelmed and under pressure (and therefore likely to make more errors with a manual process)

In this section, we have seen how automating processes in healthcare organizations can radically reduce the risk of non-compliance. Even in the worst-case scenario, when a malicious attacker does your organization damage, automation means you can be sure that, in the heat of panic, your response is level headed and effective.

Ensure compliance through automation

The Hippocratic Oath asks junior physicians to pledge that they will never share the private information of their patients. However, staying true to this pledge in the era of information technology is harder than ever. Although our technology provides a fantastic way of collecting and organizing medical information, it also significantly increases the risk that this data may accidentally be shared with the wrong people or accessed by malicious third parties.

This whitepaper has argued that, while computers and medical institutions may never be entirely safe from the risk of a breach, they can significantly boost their compliance by following best practice behaviors. When it comes to managing private information, best practice is about following processes more efficiently. And yet, because these processes are normally completed in a manual and ad hoc manner, they very often break down.

By automating the processes which will keep your organization compliant, you significantly reduce the risk of falling out of line with the law. Therefore, by implementing automated workflows across your organization, you can become more compliant and will be able to provide a transparent account of all activities relating to health information on your system should you be audited. Long term, this approach allows you to experiment and benefit from the many technological innovations that can be used by healthcare organizations, without the fear that you may get stung by a reputation-damaging fine for non-compliance.

Ready to learn more about how **the Nintex Workflow Platform** can help your organization comply with healthcare regulations?

Get in contact with Nintex today.