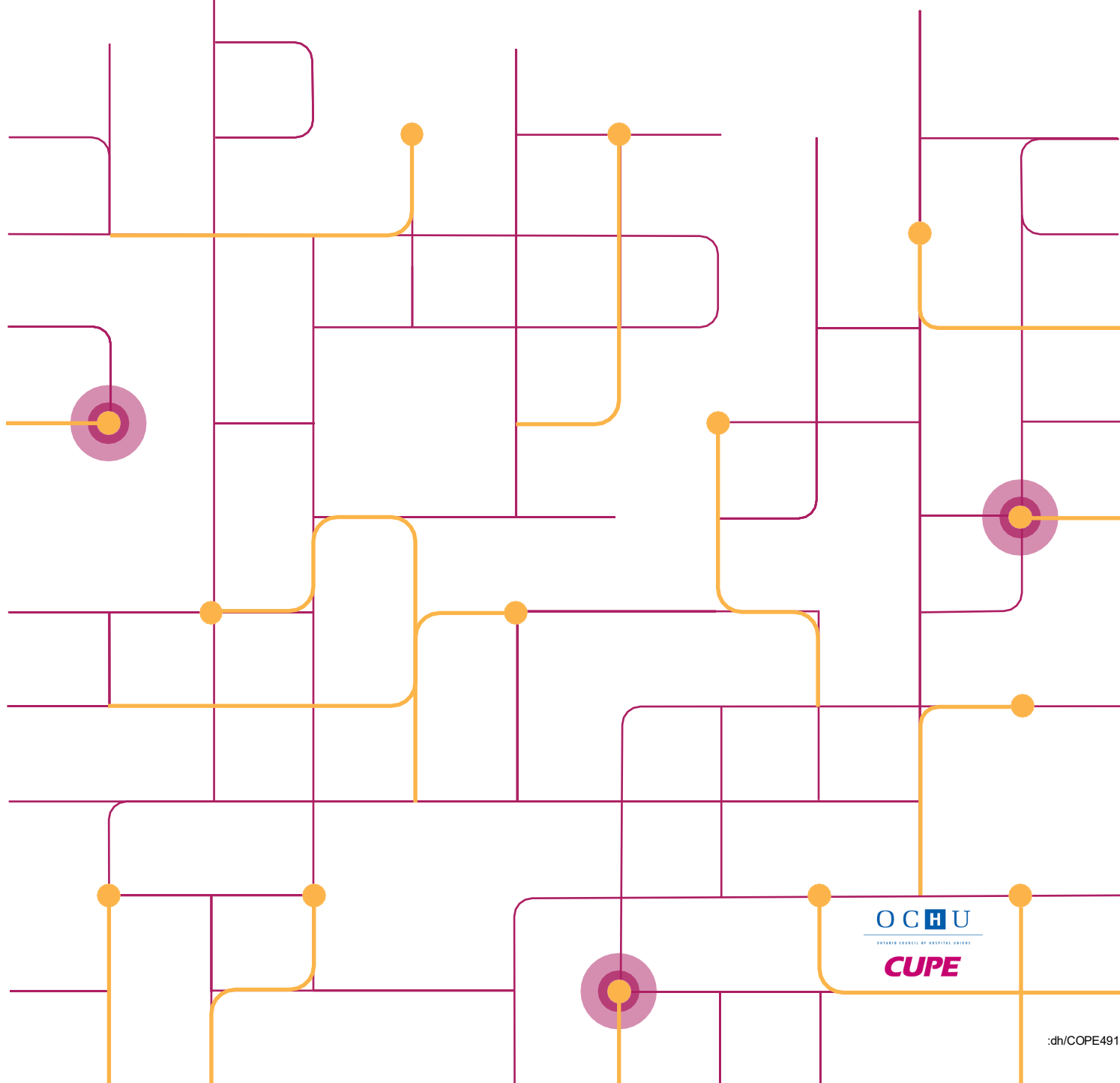


Artificial Intelligence and Technology Checklist

For Ontario Hospitals



Overview

Employers introduce technology primarily to change the process of work (reasons of production) and to change the way the workplace is managed (reasons of control). These changes often give management new ways to monitor compliance with work rules or replace and adjust human activity with mechanical or digital processes, forcing the worker to adapt to that way of working.

The hospital is no different; it is still a job site. Artificial intelligence is no different; it is still just technology. Work is a process. Technology changes that process.

As a union representing healthcare workers, we are not just fighting over dollars and cents. We are fighting for the dignity, safety, and quality of health care work itself. It is not our job to make technology work; it is to protect the interests of the patients, of the members, and of the union.

This checklist is a series of prompts, suggestions, and questions to help you and your local navigate technological change at the hospital. It is not a checklist for the employer to simply fill out but it will give you the foundations to ask the tough questions you need to make the employer stop and think

Important Collective Agreement Provisions

The OCHU-CUPE central hospital agreement includes a number of protections that can help you manage the effects of technological change and protect your members.

It is important to read the agreement language on technological change (**Article 9.13** – Technological Change) alongside other protections such as the job security and redeployment rights (**Article 9**), retraining and education provisions (**Article 9.11**), contracting out guardrails (**Article 10**), prohibitions against the reassignment of work outside the bargaining unit (**Article 11**), requirements for changes to job descriptions (**Article 20**) and the fiscal advisory committee (**Article 21**).

Article 9.13 – Technological Change

The Hospital undertakes to notify the Union in advance, so far as practicable, of any technological changes which the Hospital has decided to introduce which will significantly change the status of employees within the bargaining unit.

The Hospital agrees to discuss with the Union the effect of such technological changes on the employment status of employees and to consider practical ways and means of minimizing the adverse affect, if any, upon employees concerned.

Where new or greater skills are required than are already possessed by affected employees under the present methods of operation, such employees shall be given a period of training, with due consideration being given to the employee's age and previous educational background, during which they may perfect or acquire the skills necessitated by the new method of operation. The employer will assume the cost of tuition and travel. There shall be no reduction in wage or salary rates during the training period of any such employee. Training shall be given during the hours of work whenever possible and may extend for up to six months.

Employees with one (1) or more years of continuous service who are subject to lay-off under conditions referred to above, will be given notice of the impending change in employment status at the earliest reasonable time in keeping with the notification to the Union as above set forth and the requirements of the applicable law.

(Combined Full-Time/Part OCHU-CUPE Central Hospital Agreement, pp. 19-20)

Key Union Questions

Technology is not adopted in a vacuum. It often comes with a sales pitch on how this new tool, way of working, computer program, or new artificial intelligence agent will transform patient care, make the job easier, simplify healthcare administration. That's the "pitch".

The reality is that all changes come with disruptions, trade-offs, risks, and unintended consequences. And that is when everything goes right. Technology adoption can fail leading to health care system disruptions, more burdensome processes, wasted healthcare resources, and a degradation in our ability to deliver quality care.

As a union, we must understand the hospital's systems and any new technology to protect our members from replacement, mismanagement, violations of their rights, unsustainable workloads, and an undermining of the quality of patient care.

Before the employer adopts new technology that the union deems of interest, local unions should be able to answer the following questions (depending on the technology):

- ☐ Name and vendor of the technology and any relevant parent company?
- ☐ Copies of any procurement documents (requests for proposals, vendor proposals, contracts signed with technology providers); any new policies or changes to existing policy, and implementation plans.
- ☐ Description of the technology and its intended purpose:
 - ☐ Information provided by the vendor regarding system capabilities and limitations
 - ☐ Information about where else the technology has been adopted
- ☐ Business case or rationale for implementation for the employer.
 - ☐ What problem is this technology solving?
 - ☐ What are the expected benefits of the technology and what will be the key performance indicators (KPI) to measure whether those expected benefits are met?
- ☐ What areas, classifications and tasks will be impacted? How many members will be affected? Will bargaining unit work be reduced, reassigned, or contracted out?
- ☐ What are the timelines for implementation, testing, and deployment?
- ☐ Which manager or unit is responsible for implementation and management of the technology?
- ☐ Will the technology infringe on workers' professional judgement with patients? What rights will workers have to challenge decisions that come from the technology or artificial intelligence? Does the technology affect patient safety? If so, what risks are involved?
- ☐ What data will be collected on patients and workers? How will privacy be protected? What happens if there is a breach?
- ☐ Will patient safety be affected? If so, what risks to patient safety are involved?
- ☐ How will bias and discrimination be prevented?
- ☐ What ongoing oversight role will the union have?

The following sections include specific questions to ask depending on the technology and the union's concerns.

Job Security Section – Automation of Work and Displacement from Tasks

The technology being considered by your hospital may replace certain tasks or types of work, which in turn could affect staffing levels. Workplace technology is often adopted precisely because it replaces human labour.

It is important to look for bold statements about “time-savings”, “efficiencies”, or “productivity” that often signal the employer’s intention to change staffing levels as a result of technology adoption. These changes can sometimes be seen beforehand by the employer deciding to eliminate vacancies, understaff a unit before the introduction of a new technology or by the employer signaling there will be a hiring freeze shortly after implementation.

Considerations

- It is important that the employer understand the full life-cycle costs of any technology (what would it cost to run this technology for five years – not just the sticker price for buying the technology)
- Consider what staffing will be necessary if implementation does not go according to plan or the technology breaks down and where work may increase from inputting data, managing, or repairing the technology.
- It is important to ensure proper notification periods and long implementation timelines to protect patient care and bargaining unit work. The collective agreement has a number of provisions to protect against the loss of hours of work or any reduction in staffing.

Possible Questions to Answer

- ☐ Description of the technology and what exact tasks it will undertake
- ☐ What areas, classifications and tasks will be impacted? How many members will be affected?
- ☐ Will the employer use this opportunity to reduce staffing in certain areas, eliminate positions, restructure positions?
- ☐ Will the impact be different for some groups of employees or classifications? (for example: full-time, part-time, casual, or temporary employees)
- ☐ Will bargaining unit work be reduced, reassigned, or contracted out?
- ☐ Will there be any changes to job duties or job descriptions? (It is important to get new job descriptions if additional duties are included) Will there be new classifications? (will those positions stay in the union?)
- ☐ Are there potential contracting out, privatization, or work of the bargaining unit implications?
- ☐ What are the timelines for implementation, testing, and deployment?
- ☐ What commitments has the employer agreed to in terms of layoffs, redeployment, job security, and retraining? (Keep in mind what already exists in the collective agreement!)
- ☐ Where else has this technology been adopted? How can we learn from those who have experienced it?

Job Quality Section – How Efficiencies for the Boss can be a Headache for Workers

Technology has over the years been sold to employers and workers alike with promises to improve the efficiency of an organization and to make life easier. However, that efficiency for management has often meant speeding up the pace of work along with changing the nature of the work.

Digital technologies especially have created enormous amounts of work around documentation and data entry with staff now creating or inputting the data required for the technology to function. Time is also required to correct errors from machine output. This often creates friction as management expects – with the new technology – that the work can now be done “even faster”. This issue can be compounded as the technology leads to staffing cuts justified through cost-savings all while ignoring the new cost of the technology and additional work required to make it work.

Considerations

- It is essential to remain skeptical of claims made by technology companies and investigate whether the expectations being set by those making the technological change are realistic.
- Consider the effects of new technology not just on replacing a specific form of work but on altering the entire work process. How will everyone else be impacted and how will the work process change to make the technology fit in the hospital?
- Ensure that dialogue around technology adoption discusses the additional labour that will be required to use this technology including data entry, troubleshooting, IT, maintenance, and evaluation.

Possible Questions to Answer

- ☐ What will the effect of this new technology on workload be?
 - ☐ Will doing one task quicker/better lead to impacts on other areas of work?
 - ☐ What will occur if this technology ceases to function? For a shift, a day, a week?
- ☐ What is management trying to make possible by adopting this new technology?
- ☐ What new processes will workers need to start doing to make this technology possible? Will other technologies be required to make this viable/possible
- ☐ How much additional work could be generated to respond to time spent correcting errors from machine output?
- ☐ What risks do you anticipate if the technology barely works, half-works, and works perfectly?
- ☐ Who will be responsible for troubleshooting this technology when errors occur?
- ☐ What are the targets that management expects to meet following the introduction of this technology? Is this a realistic expectation?

Patient Care Section – Clinical Care, Patient Safety, and Professional Judgement

New technologies are being developed that provide clinical advice or direct medical interventions. These clinical AIs and algorithms carry significant risks as “AI assisted decisions” could mislead and misdirect healthcare workers, potentially triggering legal consequences for the hospital and member as well as for their licenses.

It is important to stress the legal risks the hospital may be facing with this new technology. For workers, there will be pressure to follow AI recommendations and management may treat AI outputs as superior against someone’s clinical judgement. As a result, there may be cases of discipline for overriding the AI or recommendations from a digital algorithm. We must consider what impact this technology will have on professional autonomy and scope of practice as well as who has the ultimate clinical authority.

Possible Questions to Answer

- ☐ Get a clear picture of exactly what medical functions the technology or AI will perform or support.
- ☐ Map out all the clinical decisions which may be either directed or influenced by AI.
- ☐ Proactively request risk assessments that have been on any Artificial Intelligence that provides clinical direction and document any patient safety concerns.
- ☐ Request a clear procedure for reporting errors, failures, or adverse events.
- ☐ Request a clear procedure for overriding AI recommendations and/or escalating disagreement.
- ☐ Ensure the hospital’s AI policy includes an “accountability framework” that addresses situations when AI-generated recommendations are incorrect, when human judgement takes precedence, and what protections exist for exercising professional judgement.
- ☐ Press for greater human-oversight over the inputs and outputs of the AI to ensure human review.

Surveillance Section – Employee Monitoring, Performance Management, & Labour Relations

Technology can also be deployed for the purpose of monitoring workers and exercising control over the workplace. This can include traditional methods like cameras to more modern tools like sensors and keystroke monitoring that collect data as people work. The purpose of this surveillance can vary from monitoring productivity and performance to tracking attendance and workflow.

It is very important that each method of employee surveillance is understood and that the reason and the data collected for that purpose is legitimate and reasonable. No employee should be under surveillance without their knowledge. In the age of AI, it is important to know if this data is being fed into an AI to review performance or inform disciplinary proceedings.

Employers in Ontario with 25 or more employees are required to have a written policy on the electronic monitoring of employees - hospitals are no exception.

Possible Questions to Answer

- ☐ What methods of surveillance are being used and when are employees subject to that surveillance?
 - ☐ Is the employer using any tracking technologies or location monitoring?
- ☐ What types of employee data is collected?
- ☐ For what reason is each element of data collected?
- ☐ Is the data being collected reasonable enough to suit the employer's purpose or is there overreach by the employer?
- ☐ Is the policy on employee monitoring up to date with the hospital's current methods of data collection
- ☐ How will the new technology follow collective agreement language? (particularly important for automated scheduling).
- ☐ Will this technology be used in any of the following functions:
 - Hiring
 - Promotions
 - Scheduling
 - Discipline
 - Attendance management
 - Performance evaluations
 - Return-to-work processes
- ☐ What will be the method for contesting technological decisions made without human input?

Data Privacy Section – Keeping Patient and Employee Data Safe

In today's day and age, data privacy and security are essential to protect against identity theft. Hospitals over the last decade have had a number of data breaches leaving patient and employee data to circulate online and into the hands of people who can use this information to forge identification, open bank accounts and credit cards in your name, and try to access your accounts.

Data collection should be minimized to the extent possible, collected for specific reasons, safeguarded from unauthorized access, reviewed periodically to ensure it is safe and still relevant, and anonymized to the degree possible.

Considerations

- It is the hospital's responsibility to keep the data of patients and employees safe.
- It can be helpful to think about data security in terms of the life-cycle of data. It is collected for a purpose, it is used, it is stored for future use, and ideally it is then deleted at an appropriate time. It is important to press for a shorter data retention schedule so when data is no longer useful it is deleted.

Possible Questions to Answer

- ☐ What types of data and personal information on employees is collected?
 - ☐ Who owns this data?
- ☐ What data security measures are in place to protect employee and patient data? How often will these be reviewed?
- ☐ What IT, impact or legal assessments have been done on employee and hospital data collected?
- ☐ Confirm if any third parties have access or have the potential to access employee data. If employee or hospital data is being processed by third party vendor confirm whether this data is being sold and/or this data is being used to train algorithms and artificial intelligence models.²
 - ☐ If so, what are the privacy protections for that shared data? Can individuals opt out of having their data shared? Can the hospital?
- ☐ What is the process for notifying patients, workers and the union if a digital technology is compromised? How will employees and patients be protected if their data is compromised?
- ☐ Will the data be stored within Canadian jurisdiction, so it is subject to Canadian privacy legislation? If not, in what jurisdiction will the data be stored? What are the privacy risks for data storage outside of Canada?
- ☐ What is the lifecycle for the data collected by this technology (collection, use, storage, deletion)? Does the hospital maintain control and the rights to the data at every stage or are certain rights or responsibilities transferred to the vendor. When will data be destroyed when it is no longer useful?

¹ Privacy laws in every Canadian jurisdiction dictate how the personal data of individuals must be protected.

² Employee or hospital data may be being used to train new technologies to further replace employees' work.

Human Rights Section – Managing Bias and Equity in Artificial Intelligence

Technology development often relies on data that is already generated. For artificial intelligence, this can be called “training” the AI. If there are flaws in that data or that data reflects existing inequalities, then the outputs of these same technologies can carry the same flaws or simply reflect the discrimination of the past.

The employer should be mindful of this risk and the possibility that relying on algorithmic decision-making may produce discriminatory outcomes.

Considerations

- It is important to explore whether a technology has the potential to produce discriminatory outcomes and then to question what risks the hospital is exposed to if the answer to that question is that a new technology could discriminate.

Possible Questions to Answer

- ☐ Ensure you are provided with and save all the appropriate procurement documents (requests for proposals, vendor proposals, and service agreements) agreed to by the hospital and the vendor.
- ☐ How will the hospital oversee responsible AI use and who will be directly responsible for each technology (where appropriate)?
- ☐ Will there be an audit schedule to ensure the technology is working as advertised? What criteria or benchmarks or performance indicators are being used to judge that technology? Will any evaluations or assessments be made available to the union?
- ☐ What will be the process for identifying issues and then to suspend or remove the technology if problems arise?
- ☐ Where appropriate, you may want to set up mechanisms for workers and union participation over the use of technology at the hospital.
- ☐ You will need to consider how to deal with circumstances when the employer makes system changes, upgrades, or expands the use of existing technologies.

Governance and Accountability and Union Involvement

It is important the union is involved in the process and does its due diligence in protecting members and patients from the possible harms and hazards of technology. However, it is also important that the union is not captured by this process and is seen as a “co-owner” of adopting new technology.

This mix of governing, managing, consulting and simply demanding accountability for change may vary depending on the hospital or the technology. It will be up to you as union leaders to strike that balance of protecting the members without administering technological change.

Considerations

- Technology and especially new technologies like artificial intelligence can be poorly governed without proper lines of oversight or reporting mechanisms to deal with problems. It may be beneficial to have an AI policy at your hospital to clarify responsibilities and accountabilities for those who manage and those who use AI.
- Do not forget that as members of a national union with global connections, it is likely we will have access to other hospital workers who have experience with this technology.
- It will be important to play a role in shining a light on the secrecy that some of these vendors have in order to protect their interests. Some AI vendors will refuse to explain exactly how their systems work or provide data on the risks or inner workings of the product.

Possible Questions to Answer

- ☐ Ensure you are provided with and save all the appropriate procurement documents (requests for proposals, vendor proposals, and service agreements) agreed to by the hospital and the vendor.
- ☐ How will the hospital oversee responsible AI use and who will be directly responsible for each technology (where appropriate)?
- ☐ Will there be an audit schedule to ensure the technology is working as advertised? What criteria or benchmarks or performance indicators are being used to judge that technology? Will any evaluations or assessments be made available to the union?
- ☐ What will be the process for identifying issues and then to suspend or remove the technology if problems arise?
- ☐ Where appropriate, you may want to set up mechanisms for workers and union participation over the use of technology at the hospital.
- ☐ You will need to consider how to deal with circumstances when the employer makes system changes, upgrades, or expands the use of existing technologies.

Corporate Risks Section: System Lock-in

We sometimes forget that businesses fail. A study by Statistics Canada puts the number of businesses who close their doors at a little over 10% for information technology companies every year.¹ This means that the company your hospital now relies on might disappear (vendor failure) or stop updating certain products (planned obsolescence). As we know, once something like a system or a process starts, it can be very difficult to change it – it is the same with technology services.

Considerations

- Ensure the hospital understands the risk that vendor failure poses and there is sufficient staffing, knowledge and a mapped process (critical redundancy) to keep the hospital running if it went down.
- Ensure that cost-saving estimates are not simply based on “first-contract” estimates and feature the included cost of expected customization requested by the hospital and the likely price following re-negotiation.

Possible Questions to Answer

- ☐ What is the risk of this vendor failing? Is this company financially healthy enough to exist in ten years without disruption?
- ☐ What is the back-up plan if this vendor fails to deliver updates or the product goes down?
- ☐ What is the back-up plan if this vendor fails and the technology no longer works?
- ☐ What rights does the hospital have to migrate to other vendors to provide the same service? Will the hospital be able to move their data (health records, workflow data, human resources data, etc.) to the new provider without issue?
- ☐ How will residents and workers be informed about decisions that are made based on their personal data?
- ☐ What is the risk of price re-negotiation in the future?
- ☐ What are the legal ramifications if technology failure leads to patient harm and the hospital has not made sufficient effort to anticipate technological failure?

³[A profile of corporate exits and insolvencies](#)