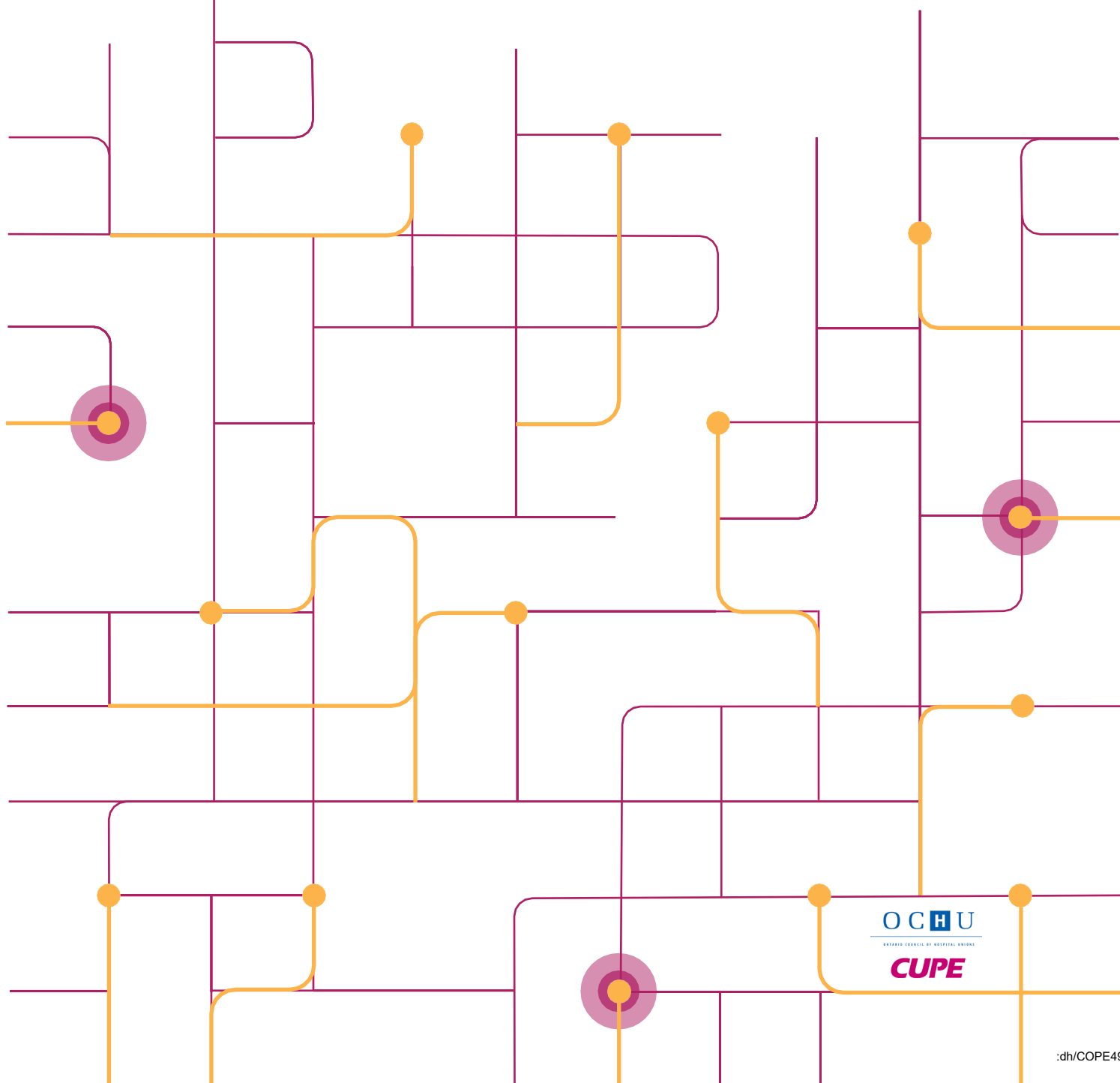


Artificial Intelligence and Technology Checklist

For Ontario Hospitals (Short)



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 effect, 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)

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

General Questions

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)
- ☐ Description of the technology and its intended purpose
- ☐ Business case or rationale for implementation for the employer.
- ☐ 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?
- ☐ 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?
- ☐ What data will be collected on patients and workers? How will privacy be protected? What happens if there is a breach?
- ☐ How will bias and discrimination be prevented?
- ☐ What ongoing oversight role will the union have?

Job Security Section – Automation of Work, and Displacement from Tasks

Statements about “time-savings”, “efficiencies”, or “productivity” 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

- Understand the full life-cycle costs of any technology -not just the sticker price for buying the technology,
- Consider what staffing will be necessary if implementation does not go according to plan.
- It is important to ensure proper notification periods and long implementation timelines to protect patient care and bargaining unit work.

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 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?)
- ☐ What are the timelines for implementation, testing, and deployment?
- ☐ What commitments have the employer agreed to in terms of layoffs, redeployment, job security, and retraining? (Keep in mind what already exists in the collective agreement!)

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?
- ☐ What types of employee data is collected?
- ☐ 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

Data Privacy Section – Keeping Patient and Employee Data Safe¹

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?

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

² Privacy laws in every Canadian jurisdiction dictate how the personal data of individuals must be protected.