



IT Systems and Patient Safety - Contracting and Governance

Michael Whitt, QC

Legal Editor, is a Partner and Co-Chair of the IT Practice Group with Bennett Jones LLP, in Calgary, Alberta.



Martin Kratz, QC

is a Partner and Chair of the Intellectual Property Practice Group with Bennett Jones LLP, in Calgary, Alberta.

Introduction

Large-scale IT systems (and some small scale systems, as well) in healthcare settings can have beneficial effects on the provision of patient care and the quality of that care. Systems, being human artifacts, may include errors and thereby on occasion introduce risks. Computer systems can introduce different types of risks, and the incidence of risk can scale up very quickly. Causes of such human generated or computer system risks can on occasion be opaque and difficult to track.

Large-scale IT systems and systems which have connectivity to other systems introduce new and different opportunities for risk, and scale the chances to propagate errors, which may escalate risk, at various stages in their development, implementation, maintenance and improvement, and use. IT systems by their nature are malleable and conformable, customizable to suit the stated requirements of their end-users, and are quite fluid, in particular when compared with other automated equipment.

The acquisition of large-scale IT systems typically is unique to the customer's needs and therefore are not "off the shelf." The systems available from Vendors are highly configurable, and specifications for any particular user organization (Health Organization) will typically be quite situation-specific.

There are many reasons for this variability,

but some important ones are: pre-existing computing or network environment; Health Organization philosophy to buy "best in breed" sub-components or "end-to-end" solutions; the nature of the Health Organization (is it a Hospital, a purchasing or network group, a health region, or a province-wide organization); culture of the Health Organization (specialist, generalist, acute or chronic care, governance structure, involvement of physician and care-giver community in IT, etc); any specific features or functions needed by local regulatory or other requirements and sophistication or experience of the personnel involved in the Health Organization's IT and clinical automation processes.

Similarly, Vendors can be widely diverse organizations, ranging from outsourcers, integration specialists, end-to-end integrated solution providers, specialist product providers, and custom developers.

In fact, in most large-scale IT procurement and implementation projects, it is likely that a number of Vendors will be involved at various points in the project, and the nature, experience, and culture of the Health Organization will change during the project's life-span.

Life-Cycle of Health Software Systems

The life-cycle of a large-scale IT system in a healthcare setting follows a typical path:

Within the Vendor's Control

- conception and design
- coding and documentation, testing
- readiness for sale

Negotiated between Vendor and Health Organization

- specification and modification to suit Health Organization environment

- procurement contracting

Performed by Vendor and Health Organization

- configuration and improvement of Health Organization computing and network environment
- installation and test of base systems
- configuration to Health Organization specifications and test
- integration with other systems within Health Organization and test
- prepare documentation and training for Health Organization users
- installation on production platforms and roll-out
- enter "business as usual" phase

Performed under Governance of Health Organization, requires Vendor co-operation

- continuous use and maintenance
- system capabilities beyond initial automation are implemented
- new capabilities and uses are conceived, implementation processes carried out
- new components are added, other systems are connected, other users are served, etc.
- eventual decommissioning
- safe transition to new systems
- safe and secure removal, storage, destruction of data and hardware

Within this widely accepted model to describe and think about large-scale IT systems in healthcare, it is convenient to think about 4 main phases in the lifecycle of such systems:

1. "Pre-Marketing" Phase: conception, design and build by Vendor of base systems.
2. "Procurement and Contracting" Phase: including determination of technical specifications of beginning and initial installed state of system,

configuration and training requirements to implement, interconnection and interoperability requirements with other systems, expected growth-path and user types and numbers, initial service levels sought, system useful-life, and suitable test-acceptance cycles, dispute identification, documentation and resolution mechanisms, and suitable financial gain and risk-sharing business models (which are likely different for each phase during the buy/implement/operate parts of the cycle). Note that this portion of the lifecycle precedes any actual implementation or installation work.

3. **Implementation Phase:** Configuration of Health Organization environment, installation, configuration and test of IT system, integration with other Health Organization systems (and interfaces with outside systems), documentation and training of Health Organization personnel, test and rollout.
4. **Business as Usual Phase** (including decommissioning of the former system in favor of new system at end-of-life): continuous use and maintenance; system capabilities beyond initial automation are implemented; new capabilities and uses are conceived, implementation processes carried out; new components are added, other systems are connected, other users are served, etc.; eventual decommissioning of the new system.

Discussion of Each Life-Cycle Phase:

It is important at this stage to remind ourselves of the purpose of this examination: to identify risks to patient safety at various stages of the life-cycle of large-scale health software systems, in order to identify the most appropriate types of mechanisms to control and mitigate those risks.

Pre-Market and Market-Readiness

Where the system is under near absolute control of the Vendor, it is appropriate to push obligations to protect patient safety onto the Vendor. At the “pre-market” stage, mechanisms which are appropriate may include external regulation, but surely includes obligations that the Vendor use reasonable efforts to design the system to function as predictably as possible, to test the system for accuracy and expected operation before selling or licensing it, and to document the system so that safe modes of operation are detailed, and known risks in operation or deployment are identified.

Associated with this aspect are reasonable warranties and representations within the procurement contracting documentation that the system, as specified and supplied,

will perform in accordance with the functional aspects documented. (more below).

In situations where the health software is adjunct to, or a necessary component of, a medical device, or is itself a medical device, this is an appropriate spot to regulate quality and efficacy in operation to match labeling and descriptive documentation by requiring compliance with things like Health Canada’s Medical Device Regulations. Having said that, at this point in history, these large-scale IT systems do not appear to fall under Health Canada’s jurisdiction (to regulate them as medical devices).

There is a heightened level of activity within various regulatory agencies to begin to understand how and where their regulation of systems as devices is or can be appropriate, and whether there are additional regulatory mechanisms required (such as “meaningful use” in US parlance, or “Patient Safety Risk Management” in NHS/UK parlance). ISO standards bodies, in particular TC215’s Expert Working Group on “Standards Requirements for Enabling Safe Health Software” (current working title), are working on identification of the current lay of the land in this realm.

Difficulty arises when the Vendor alters aspects of its designed and coded system in order to satisfy Health Organization configuration requirements, or when Health Organization users modify their actual uses of the system to be outside of protocols and processes designed and approved by the Vendor. (more below). In those cases, the control over the system arguably becomes a shared responsibility, the number of system variants introduced by user customization becomes extreme, and pure compliance or licensing obligations will probably not be either appropriate or sufficient to ensure optimal patient safety.

To the stage of “market readiness”, before the system is personalized, customized or configured to suit a particular Health Organization, the management of patient safety risks is under the control of the system Vendor. If more than one Vendor is involved in an inter-operative system, responsibilities become shared and less obvious and need to be managed.

Procurement and Contracting

In large system procurement exercises, it is typical that one or more RFP documents are provided by the Health Organization to the Vendor community. Prior to the initial RFP, the Health Organization will typically have considered its needs and desires for new systems, and may have done some market review of Vendor offerings, and

hopefully will have reviewed other similar systems implemented successfully by similar third party health organizations. The RFP process will run its course through one or more iterations, and eventually a successful Vendor (or Vendor group) will be selected from the field of respondents. Procurement is a very sensitive topic in large system acquisitions, and in particular in healthcare. It is becoming increasingly rule-bound and process-bound. These explicitly prescribed purchasing rules are designed to ensure fairness of treatment to Vendors and avoid problems of favoritism and bias, as well as to ensure that market forces (competition) motivate best pricing and quality. The rules of procurement are beyond the scope of this article, but cannot be ignored or avoided. The procurement process itself does not protect patient safety, but it is possible to build protective mechanisms into the specifications and contract documents associated with the transaction(s).

Once a Vendor (or Vendor group) is selected, detailed contract documents are then negotiated and prepared. The goal of the contract document is essentially two-fold: to describe in as much detail as is possible the obligations of each of the parties to deliver goods and services to specified degrees of quality, service levels, and timeliness and to pay for those things when they are delivered or are reasonably acceptable, and to provide the constitutional framework for a long-term mutual dependency relationship which is built to work through uncertainties and circumstances which can be imagined but not resolved at the contract’s date and to resolve conflicts which will inevitably arise; this will include things like change-control processes, service-level adjustments and bench-marked pricing adjustments, among other things.

Within the more concrete portions of the procurement contract dealing with specific obligations, one would expect there to be patient safety-specific obligations for both parties to report operational errors to the other, or to some common report forum, obligations to report bugs, workarounds, failures, alteration of work-flow, and other things or occurrences which would affect patient safety within an operating health software system. One would also expect obligations to co-operate to identify and isolate system functions which produce results which affect patient safety, and to escalate repair, workaround, modification, testing and rollout of modifications to mitigate the risks. One should also expect some exceptions to confidentiality obligations to permit the parties to communicate problems which may affect unrelated third parties using other similar

systems, in order to assist in the safety of patients who may be affected by those other systems; similarly, workarounds and fixes should probably not be proprietary without permission to roll them out to the benefit of those other patients.

Within the governance/constitutional portion of the contract, attention should be paid to the constitution of a Software Oversight Committee or similar multi-party committee which is authorized and mandated to receive information about system problems affecting patient safety, and to make decisions about system implementation, change, and operation to mitigate patient safety issues. This body should not be subordinate in the Health Organization to those in charge of implementation, but rather should be a permanent oversight function with authority to control mitigation of patient safety risk introduced by system implementations, both before and after “go-live.”

Installation, Customization, Implementation and Training, Go-Live

The roles of the Vendor and the Health Organization should be knowable by reference to the Procurement Contract documents, perhaps in association with Change Orders which have been approved as the extent and details of the work became known during this phase, post-contract (this is typical). In particular, with respect to controlling and minimizing risk to patient safety, system test protocols and procedures should have been designed. Implementation risk typically arises from: failure to check data mappings from other systems to this system, informal and undocumented staff-invented work-arounds for alerts or other system safety functions, poorly ordered menu lists or other awkwardly designed user interface elements, or local changes with unintended consequences to data stores or other connected systems, inadequate documentation or instruction, mismatch between actual work-flows and automated processes; different and non-obvious approvals processes, and the like (tractable). These types of risk-inducing failures are identifiable and avoidable if appropriate design and documentation controls are in place, and if interface best-practices are followed, but most specifically, if adequate testing is designed into the implementation phases prior to exposure of live patients to potential risk.

During the implementation and installation phase, until go-live, the parties are acting in mutual reliance, and so the constitutional elements of the procurement contract documents, including language which elevates the importance of patient safety

and structures which provide oversight to identify and manage risk to patient safety, are most important.

The details of acceptance testing and phase-gating within the implementation and roll-out will likely be modified after the procurement contract is executed, and the modifications will be found in technical documentation within Change Order forms – having said that, if patient safety has been elevated in importance as a driver behind the Health Organization’s choice of Vendor and project specifications, and there are appropriate governance bodies controlling actions or functions which pose risk to patient safety, it is more likely that concerns about mitigation of risk to patient safety can affect deployment schedules, activities, and costs.

Business As Usual

First, it is important to recognize that unlike our experience with other large-scale projects, such as highways and bridges, “business as usual” in large-scale healthcare IT systems is tremendously flexible. Network, hardware, computational power, storage capacities, user demographics, system capability, information management theory, and the practice of medicine itself changes and is changed by the use of IT.

Thus, conceiving of management of patient risk as a static task is inappropriate, and the governance and values structures in the initial procurement contract documents become the most important risk management tools, more important than most specific rules. Those governance tools will be amended from time to time by alterations to system specifications, service level agreements, scope documents, operating protocols, work-flows, data interchanges, messaging, and on and on.

Care needs to be had at major systems change events, such as the introduction of CPOE, or integration of evidence-based workflows, or moves to virtualization. These major events can change the Vendor/Health Organization relationship, introduce new parties or players, or elevate or disenfranchise different groups. Those changes can affect patient safety, and should be planned and effected in the context of respect for patient safety.

The main exception to the general fluidity of the contract in this phase might be the end-game...the termination of the system and the relationship between the Vendor and the Health Organization, and the consequences on termination. One should expect there to be obligations in the basic contract documents dealing with how termination can occur, who can trigger the

end of the relationship and how must that be done, and most importantly, how the “business as usual” operation of the system can be unwound and, if desired, transferred to another system or another operator, while guarding the safety of the patients the system serves, and the integrity, security, privacy and safe destruction, if desired, of the information within the system.

Thought might be focused, periodically, on the ownership of jointly made system or operational improvements, and how those can be shared more broadly with other Health Organizations, and how costs and gains might be recovered or recaptured.

Summary

In conclusion, it seems prudent to include a review of the life-cycle of health software in our understanding of patient safety and the regulation of risks which impact patient safety. The thesis of this article is that there are four different phases to the life-cycle of health software: (1) Pre-market conception, development, coding and documentation by the Vendor; (2) Procurement, including development and negotiation of specifications and contracts documents; (3) Installation, customization, training and implementation to acceptance testing; and (4) Business as Usual, to end-of-life.

Each stage of this lifecycle presents differing types of risks to patient safety, and responsibilities for management of those risks should typically relate to the parties’ differing ability to identify, control and manage those risks.

Since this is written from a lawyer’s perspective, it should not be surprising to find a focus on the Procurement Contract negotiation and documentation as a leverage point to positively affect patient safety risk, in particular in two ways:

1. By proscriptive language detailing and defining specifications, acceptance tests, configurations and service level expectations; and
2. By constitutionally building a relationship between Health Organization and Vendor with specifically stated goals which elevate patient safety as a primary concern, and which provide for organized change controls and dispute resolution functions, but also provide obligations on all parties to identify and report instances of increase to patient risk associated with the system and work together to reduce the potential for harm.