



INFONAUT

evidence-based infection control

Infonaut is a privately held Canadian company born out of Ontario's SARS crisis, and dedicated to evidence-based solutions for infectious disease surveillance to control and stop superbug infections in hospitals in an effort to prevent infectious deaths and morbidity.

Our solution, **Hospital Watch Live**, helps solve the mystery of how healthcare acquired infections move about a facility. It tracks, in real time, the vectors and risks of communicable infectious diseases to understand and help break the chain of infection transmission in hospitals. We bring a location aware enterprise risk management approach to improving quality. The outcome is a dramatic improvement in patient and workplace safety resulting in massive savings.

Hospital Watch Live easily integrates into existing hospital systems. The deployment of a Real Time Location Systems (RTLS) into clinical environments allows hospitals to track and store all movement, contact and interaction of patient, staff and assets. This provides instant, risk-rated contact tracing, with predictive analysis of patterns and disease reservoirs.

There are universally accepted techniques and methods based on an understanding of 'history of location' and 'transmission' common to diseases surveillance and infection control that form the basis for the science of epidemiology. For the first time, Infonaut uniquely automates and applies these techniques inside the hospital via a patented platform and process to provide superior infection control that has global applicability.

Infonaut has received recognition and acknowledgement from international leaders in hospital infection control, leading global hospital technology vendors, trade journals, mass market publications and globally recognized market analyst firms.

Our solution was designed from the initial concept with respect for privacy and ethics. We believe that our commitment to the Privacy By Design philosophy represents a major competitive advantage.

Here is how Infonaut addresses the [7 Foundational Principles](#) of Privacy by Design (PbD):

- **Proactive not Reactive; Preventative not Remedial**

We adopted PbD principles in 2008 before we started development of our solution, **Hospital Watch Live**. From voluntary participation, to anonymous group level reporting, to adoption of a change management process that encourages group responses, a privacy-based approach will help resolve issues and problems of hospital superbugs and infection transmission that our platform identifies. A rigorous Privacy Impact Assessment is completed by the hospital and our staff prior to deploying our solution - and proactively assesses risk before final approval is provided by the hospital to proceed.

Additionally, as a surveillance solution, we deploy only in areas where we believe will have an impact. For instance, we do not include staff-only common areas for surveillance coverage - and users are openly informed about where they can be tracked and where they will not be.

In instances where there is some question to the use of our solution and the outcomes desired, we default to considerations that respect the privacy of users until there is consensus from staff, management and privacy experts to proceed.

Our solution's success is ultimately predicated on the sustained adoption by staff and patients/families in a hospital setting. If the covenant of trust is broken and users choose not to participate, we understand that overall success will be compromised. Therefore, it is in our best interests to ensure that our respect of their privacy ensures ongoing support and adoption.

- **Privacy as the Default Setting**

The default setting of our solution reflect a commitment to privacy first and foremost. This includes carefully identifying information that is collected is the minimum required, assigning role-based access prior to deployment, voluntary participation of staff, proactively providing information on the scope of deployment and the scope of use, use of the information, and change management.

- **Privacy Embedded into Design**

Recognizing that we were developing a surveillance solution, the principles of PbD were adopted prior to development. All stages of our development considered privacy as one of the core principles of design.

These principles are shared with users prior to deployment to ensure that they understand the data collected and scope of use before they voluntarily participate. Additionally, we also instruct users on methods to defeat the system so that in cases where they do not feel that privacy is being maintained, they can opt out at any time.

- **Full Functionality — Positive-Sum, not Zero-Sum**

The business and clinical value of our solution positively impacts management, clinical staff, environmental staff/contractors as well as patients/families. We deliver value to all these stakeholders while respecting the privacy and security of each.

Ongoing commitments to maintaining this covenant with the stakeholders is the only method that we believe will encourage ongoing adoption, sustainability and ongoing success.

- **End-to-End Security — Full Lifecycle Protection**

Our solution is deployed only after a Privacy Impact Assessment and Threat Risk Analysis is completed by hospital staff, including experts in system architecture, data security, privacy, as well as management .

The information collected remains within the hospital and is subject to the same rigorous privacy standards as all hospital systems. The data is analyzed and presented at an aggregated level under rigorous role-based security and access privacy levels so that the appropriate audience is given the relevant information.

Ongoing analysis of the data to create new learnings and research of how infections are transmitted in a hospital will use anonymized data to ensure that privacy and data security is respected.

The lifecycle of the data is defined by the scope-of-use, primarily being research and latency of disease.

- **Visibility and Transparency — Keep it Open**

Participation by staff is fully voluntary and patients are given the option of not being included. The solution's scope-of-use is provided to staff and patients prior to their participation so that they can make a fully informed decision prior to participating. Users are instructed on how to defeat the system as part of the initial training, if they feel if their privacy is not being respected.

The results from our solution are then provided back to the group on an anonymous basis so they can make informed decisions regarding changing group behaviour to practices and interventions that should reduce infectious morbidity and mortality. Ultimately, we believe that the carrot is a much more effective tool than a stick.

- **Respect for User Privacy — Keep it User-Centric**

We have designed our solution to be user-centric. The system conforms to the user - we do not ask the user to conform to the system. No additional tasks or processes are requested when the solution is implemented. We ask that hospital staff and patients go about their normal business.

Any changes to processes are designed and implemented based on user-feedback Maintaining privacy is one of the primary considerations when new processes are considered prior to implementation.

For additional information about Infonaut please visit www.infonaut.ca