Syndromic surveillance for health information system failures: a feasibility study

Mei-Sing Ong, Farah Magrabi, Enrico Coiera

ABSTRACT

Objective To explore the applicability of a syndromic surveillance method to the early detection of health information technology (HIT) system failures.

Methods A syndromic surveillance system was developed to monitor a laboratory information system at a tertiary hospital. Four indices were monitored: (1) total laboratory records being created; (2) total records with missing results; (3) average serum potassium results; and (4) total duplicated tests on a patient. The goal was to detect HIT system failures causing: data loss at the record level; data loss at the field level; erroneous data; and unintended duplication of data. Time-series models of the indices were constructed, and statistical process control charts were used to detect unexpected behaviors. The ability of the models to detect HIT system failures was evaluated using simulated failures, each lasting for 24 h, with error rates ranging from 1% to 35%.

Results In detecting data loss at the record level, the model achieved a sensitivity of 0.26 when the simulated error rate was 1%, while maintaining a specificity of 0.98. Detection performance improved with increasing error rates, achieving a perfect sensitivity when the error rate was 35%. In the detection of missing results, erroneous serum potassium results and unintended repetition of tests, perfect sensitivity was attained when the error rate was as small as 5%. Decreasing the error rate to 1% resulted in a drop in sensitivity to 0.65–0.85.

Conclusions Syndromic surveillance methods can potentially be applied to monitor HIT systems, to facilitate the early detection of failures.

INTRODUCTION

In recent years, healthcare delivery has become increasingly dependent on health information technology (HIT). HIT has tremendous potential to improve healthcare quality. However, its use has been associated with unintentional consequences that could potentially lead to patient harm. In 2011, the US Institute of Medicine called for urgent action to address the risk of HIT on patient safety. Our recent analysis of incident reports in the USA and Australia showed that simple software faults or deficiencies in software interfaces may impact on patient safety.

A different type of risk posed by our increasing dependence on HIT is the potential implications of cybercrime on healthcare infrastructure. Attacks could alter or destroy individual medical records, alter computer-based prescriptions to life-threatening doses and disrupt delivery of vital medical services. Several cases of cybercrime against healthcare systems have already been reported, and the frequency of such incidents is only likely to grow in the future.

Despite the risks associated with the use of HIT, there is currently a lack of infrastructure for managing and monitoring the safety of HIT systems. Existing methods for monitoring harm caused by HIT systems are minimal, mainly relying on voluntary reporting using generic patient safety adverse events reporting systems. Information gathered by such systems does not provide a numerator or denominator, so the true incidence of problems cannot be realistically assessed. There is a high degree of variance in reporting of HIT incidents, as users often do not realize the extent to which software determines many of the functional and performance characteristics of a system. Furthermore, many software vendors legally limit the ability of their clients to report these types of errors publicly. As a result, HIT problems are largely left undetected, or detected only after enough evidence accumulates. This process can take a long time, with costly implications on patient safety.

Ensuring the safety of a HIT system is a challenging task. Software is inevitably complex, and errors can be difficult to detect. Most health information systems consist of multiple disparate components. Individual components can interact to produce system behavior in ways not intended by the original designers. Compounding the problem is the complexity of healthcare organizations. Emergent behaviors that arise from these complex interactions cannot be determined analytically, and are only evident when the system is deployed in the real world. Therefore, the events that are most likely to harm patients will occur after HIT systems are implemented, often from unpredictable chains of low-risk events. There is therefore an urgent need for innovative techniques to monitor the safety of HIT systems post-deployment. Increasingly, researchers are calling for active monitoring of HIT systems.

Early detection of health information system failures through syndromic surveillance

In the field of biosurveillance, syndromic surveillance has been used for the early detection of disease outbreaks. The method involves analyzing real-time information about health events that precede a confirmed clinical diagnosis of a disease, in order to detect signals that might indicate an outbreak. This allows for much earlier notification of potential outbreaks, providing public health officials with the opportunity to respond earlier and thus more effectively. For example, abnormally high emergency department visits have been used as an early signal for disease outbreaks.
Developing a syndromic surveillance system

Our study follows the same approach used for building a syndromic surveillance system for disease outbreaks, consisting of the following steps: defining syndromes; modelling baseline profiles; defining detection algorithms; and model validation.

Defining the ‘syndrome’

The first step of developing a syndromic surveillance system involves selecting the appropriate indices to be tracked. If we consider a HIT system as a black box that delivers data to a human operator, then its performance can be judged against two broad criteria—data quality and data availability. Data quality reflects a system’s capacity to capture faithfully, store and then retrieve data. Data availability reflects the capability of a system to communicate those data in a timely manner. Detection of data availability problems, measured in message latency or system up-time, is a well-established domain, and many network monitoring tools are in wide use. Problems with data quality are, however, harder to detect, given that there is often a semantic component to the task, and detecting whether the intended meaning of a data item has changed requires an approach that in some ways models the expected values of data items. In this study of HIT failure detection, we thus focus on the development of simple methods that can assist in the surveillance of problems in clinical data quality.

Problems in clinical data quality can manifest in one of four ways: (1) data loss at the record level (ie, loss of laboratory record created by a provider); (2) data loss at the field level (ie, loss of data stored as a field within a laboratory record); (3) erroneous data being introduced into existing records (ie, data entered by a provider differ from the data being stored or retrieved); and (4) unintended duplication of data (ie, duplication of existing records not manually created by a provider). Collectively, these symptoms define the syndrome for LIS failures.

In order to capture these four classes of failure symptoms, we chose to monitor the following indices:

1. Total laboratory records created in a given time frame—an unexpected drop in the number of test records created provides an indicator for data loss at the record level.
2. Total laboratory records with missing results—an unexpected increase in the number of tests with missing results field provides an indicator for data loss at the field level.
3. Average test results for individual tests (serum potassium was selected as a proof of concept)—an anomalous shift in the average level of serum potassium across all patients could signify that the data integrity of the LIS has been compromised.
4. Total number of tests of any types performed on the same patient within 24 h of the same test being performed—a sudden increase in the number of duplicated tests requested on the same day is an indicator that test requests may unintentionally be duplicated.

The underlying premise is that unexpected changes in these indices are strong signals for potential HIT problems. For instance, at any point in time, there would be a baseline level of missing results (due to pending test results) and duplicated tests (due to the need to repeat tests) that are clinically warranted. HIT failures resulting in the loss of test results or spurious duplications of tests would manifest as deviations from the baseline level. Likewise, there are inherent fluctuations in the number of new records and the average results for serum potassium. The detection goal is to separate the error signal from the noise caused by natural variations in the data.
Modeling baseline profile
To detect unexpected changes in the indices, we must first define normal behavior. We divided our dataset into two—we used approximately two-thirds of the dataset as a training set (including all tests performed between February 2011 and October 2011), and the remaining third as a test set (including all tests performed between November 2011 and February 2012). Using the training dataset, time series models for the indices were independently constructed. As a first step, principal Fourier component analysis was performed to identify the main periodicities in the data. When periodicities were found, the data were modeled as a non-stationary process with periodic mean value and periodic SD. 21 When periodicities were absent, the data were modeled as a stationary process with a constant mean and SD. Accordingly, the number of test records created, the number of records with missing tests results, and the number of duplicated tests were modeled as non-stationary processes. The level of serum potassium was modeled as a stationary process. These models represent the natural variations inherent in the data, and significant deviations from these models are signals of a potential anomaly. To facilitate the timely detection of abnormal patterns, the indices were sampled on an hourly basis.

In order to confirm that the baseline models did not contain unexpected variations, an iterative process of testing for statistical control was applied. This involved searching for data points in the training set that did not lie within the statistical control limits (defined as 3 SD above or below the process mean), identifying the causes of these unnatural variations through qualitative assessment of the outliers, and removing them from the dataset. 22 23 This is a critical step, because without bringing the baseline process into a state of statistical control, we cannot make any valid probability statements about the future predicted performance of the process. 24 A process operating at or around a desirable level or specified target with no assignable causes of variation is said to be in statistical control. 24

Defining detection algorithms
To detect unexpected variations caused by LIS failures, Shewhart statistical control process charts were used. 25 A control chart consists of three components: the center line (CL), the upper control limit (UCL) and the lower control limit (LCL). Data that fall outside the control limits are markers of unexpected patterns that could be indicative of a HIT system failure. As the aim was to detect variations from the process mean, an x-bar control chart was used, in which CL was defined to be the mean of the baseline model; UCL and LCL were set as 3 SD above and below the mean, respectively. Alarms were triggered when an observed data point was found to be above the UCL or below the LCL.

We also applied additional detection rules to improve our model sensitivity. These included:

1. Two out of three successive points more than 2 SD from the mean on the same side of the CL.
2. Four out of five successive points more than 1 SD from the mean on the same side of the CL.
3. Six successive points on the same side of the CL.

Therefore, in the final model, an alarm was triggered when a data point was either found to fall beyond UCL or LCL, or when any of the above detection rules was satisfied. Normality of data was tested and confirmed by the Kolmogorov–Smirnov test, using SPSS V20 (p<0.001).

Model validation
During the study period, the only known HIT system failure was a network problem between 5 March 2011 and 22 March 2011. This data availability incident substantially reduced the speed of the hospital network. However, it did not affect the quality of the data, which is the focus of this study.

In the absence of real-world system failure data, a series of simulated experiments was carried out to validate our models. This involved simulating scenarios representing the four symptom classes described above:

1. To simulate data loss at the record level, laboratory records in the LIS were randomly deleted, and the ability of our model to detect these losses was assessed.
2. To simulate data loss at the field level, test results in existing records were randomly deleted.
3. To simulate erroneous data at the field level, wrong results were injected into existing records. As a proof of concept, the simulated scenario involved doubling the serum potassium value in existing records.
4. To simulate the unintended duplication of test records, duplicated test requests for a patient on the same day were generated and injected into the LIS.

Error rates and duration
The number of records affected in each failure scenario was determined by an hourly error rate. For instance, at an error rate of 1%, the loss of test records was simulated by randomly removing 1% of the test records in a given hour. Likewise, at the same error rate, duplication of tests was simulated by randomly duplicating 1% of existing test records in an hour. Several error rates were applied to examine the effectiveness of the model in detecting errors of varying sizes (1%, 5%, 15%, 30%, 35%).

For each error rate, 100 episodes of the same failure scenario were injected into the test dataset. The starting date and hour of the error episodes, as well as the actual records affected, were selected using a computerized random number generator. Each episode lasted 24 h, during which the error rate was held constant. The small error rates and duration were selected to test the ability of our model to detect small and short-lived failures that often precede more catastrophic failures.

Performance evaluation
The ability of the model to detect the failure within 24 h, at a given error rate, was assessed using the standard metrics of sensitivity, specificity and the timeliness of detection. For the purpose of this study, we defined sensitivity to be the proportion of failure episodes that were correctly identified out of the total simulated failure episodes at each error rate (ie, the number of failure episodes correctly identified/100 simulated episodes). Specificity was determined by measuring the number of hourly false alarms over the entire test dataset (in which specificity is 1–false alarms). The timeliness of detection was defined as the number of hours required to detect a failure episode since its onset.

RESULTS
Baseline profiles
The number of new laboratory records created showed weekly and daily periodicities (figure 1). A higher number of records was created on weekdays compared to weekends. On a given day, the number of records being created peaked around 10:00 hours, decreasing steadily through the day, and gradually increased again at around 05:00 hours the following day. The
number of records with missing results and the number of duplicated tests were strongly correlated to the total volume of test orders, yielding a Spearman’s correlation coefficient of 0.757 and 0.969, respectively (p<0.001). Therefore, similar daily and weekly periodicities were found. The average value of serum potassium results did not appear to exhibit any periodicities, remaining relatively constant at approximately 4.19 mmol/l, with a SD of 0.19. A number of records in the training set showed an abnormally high serum potassium level (>20), causing the time series to appear statistically out of control. These values were treated as abnormal variations, and were excluded from the baseline model. A total of 111 records was excluded (0.06% of the total records). We were unable to ascertain the causes of these variations definitively. Possible reasons include problems with the specimen caused by hemolysis, and data entry error. As the results of tests were manually entered by laboratory scientists, it was likely that decimal places were mistyped (eg, a value of 4.3 was mistyped as 43).

Model performance
Model sensitivity and specificity

The sensitivity of the models in detecting simulated failures is shown in figure 2. Of the four indices, data loss at the record level was the least sensitive. At an error rate of 1%, the model was able to detect 26% of simulated record losses. Detection performance improved with greater simulated error rates, with sensitivity increasing to 100% when the simulated error rate was 35%. The remaining indices performed well at all error rates, achieving a perfect sensitivity when the error rate was 5% or more. At an error rate of 1%, 65% of missing results were detected, 70% of erroneous serum potassium values were detected, and 85% of duplicated tests were detected. In all cases, a specificity of 0.98 was achieved when the detection algorithms were applied to the test dataset without any simulated failures. This produced approximately two to three false alarms per week.

Figure 1 Baseline profiles.

Figure 2 Model sensitivity.

Figure 3 Timeliness of detecting loss of laboratory records.
Overall, most simulated failures were detectable within the first few hours of onset, and the timeliness of detection improved as the magnitude of simulated failures increased (figures 3–6). Of the four indices, serum potassium results were the most responsive index, with 75% of simulated failures identified in the first 6 h when the error rate was 5%, more than 88% of simulated failures identified within the first hour when the error rate was 15% or more, and 100% of failures identified within the first hour when the error rate was 30% or more. The timeliness of detecting missing results and duplicated tests was also comparable, achieving approximately a 70% detection rate in the first 6 h when the error rate was just 5%, more than 80% when the error rate was 15% or more, and attaining a perfect detection rate within the first 2 h when the error rate was 30% or more. The timeliness of detecting data loss at the record level was poorer compared to the other indices. At an error rate of 35%, 22% simulated failures were detected in the first 2 h, increasing to 55% at the fourth hour, 94% at the 12th hour, and 100% at the 24th hour.

**DISCUSSION**

In this study, we have adopted concepts from syndromic surveillance to construct models for detecting HIT system failures. The results were promising, showing the potential for employing such approach in a real-world setting. Most simulated failures were detected within hours, while maintaining a specificity of 0.98. The sensitivity of the models and the timeliness of detection improved as the magnitude of the failure increased.

We selected four indices to track the health of a LIS, each representing a distinct type of error. The surveillance system could be easily expanded to include multiple indices for each class of error. For example, to enhance the capability of the system in detecting data loss at the field level, other fields can be monitored alongside the results field. This will ensure that data loss in other fields will also be detected by the surveillance system. Similarly, additional test types may be monitored in addition to serum potassium.

An important factor that dictates the sensitivity of a surveillance system is the sampling time frame. In general, the shorter the sampling period, the more sensitive the system becomes. However, this may also increase the false alarm rate. In our study, we chose to sample our data on an hourly basis. Our choice of sampling period appeared effective, with the model achieving very high specificity and sensitivity in all scenarios.

A key motivation for any surveillance system is that it can perform better than manual detection. While we do not have data to compare the performance of our system with manual detection, it is reasonable to assume that HIT system failures, especially failures of small magnitude, can easily go undetected. In the case of a LIS, there are often minimal interactions between pathology departments and inpatient wards, and problems with the information system may be wrongly perceived as process or administrative delay. For instance, loss of test results caused by system failures may not be detected as physicians could misperceive the loss as results still pending. Therefore,
intermittent HIT system failures that diffuse across multiple wards would be unlikely to be discovered until the problem becomes more widespread. Having an automated surveillance system that is capable of detecting process deviations can provide a much earlier and reliable warning system for potential problems.

What are the advantages and drawbacks of this approach?

Surveillance of information systems is by no means a new concept. In fact, automated surveillance is a prerequisite for any fault-tolerant systems. Traditionally, real-time surveillance of information systems involves tracing the runtime properties of a system to identify possible causes of failures. Common variables monitored include network traffic, event messages between components, system resources consumption, and log error messages. Therefore, the surveillance system is tightly coupled to the operating system and the software being monitored. Fault detection algorithms would have to be tailored to a specific system. Managing such a system can be challenging and costly, as the behavior of the observed variables may evolve over time, as new components are being added, and old ones removed. Furthermore, detailed programmatic knowledge of the software is often necessary to develop such a system. Therefore, the approach may not be practical in a complex healthcare setting, which is often made up of a combination of homegrown and commercial software components. Our approach differs from the traditional methods. Rather than tracing the runtime properties that define a system, we monitor the health of an HIT system by tracking the clinical data managed by the system. This approach has the advantage of being ‘system agnostic’, as it is not affected by the dynamic and complex relationship of software components. This therefore greatly enhances its generalizability and manageability. An added advantage of using clinical data is that the data are already available, thus reducing the effort and costs associated with introducing new data collection processes.

A notable strength of using statistical process control is that the control limits of a process are defined based on local statistical properties (ie, SD and variance), rather than a predefined reference range. This method can thus be locally adapted to monitor data elements of different distributions, without having to understand the underlying meaning of the data.

There is an obvious drawback to this approach—we cannot be certain that the unexpected patterns in the observed data are indeed linked to HIT system failures. The data can be subjected to influences that have nothing to do with the underlying HIT system. For example, a breakdown in laboratory equipment may cause a sudden shift in the average serum potassium level; a change in hospital process may result in a sudden increase in unintentional duplicated tests. This problem is not unique to our system. At the expense of facilitating the earlier detection of an event, syndromic surveillance data are generally imprecise measures of the event. The system is designed to detect unexpected variations, but it does not provide insight into what causes the variations. Further in-depth investigation would be required to uncover the actual cause. For this reason, syndromic surveillance of HIT systems is not intended to be a replacement for traditional approaches of analyzing system variables. Rather, it complements them. Aggregating information provided by different surveillance approaches will improve error diagnosis and detection. An optimal system might be one that integrates data from multiple sources, potentially increasing investigators’ confidence in the relevance of an alert from any single data source. It should also be noted that the control limits of a surveillance system must be continuously re-evaluated, as the data may shift over time for a number of reasons. Failure to do so may result in the suppression of future alerts.

Limitations and future studies

Our study is an early stage feasibility study, and therefore the findings should be interpreted within this context. There are several limitations in our study. As we have built our model based on one hospital, our results may not be generalizable across other settings. It also remains untested whether this approach of surveillance would apply to other more complex HIT systems. However, given that our approach is designed to model local statistical distributions of data values, the method should readily be applied at different institutions and on different systems.

We were also constrained by the limited dataset. Baseline models for detection systems should ideally be based on many years of historical data. In our study, we divided a 1-year dataset into separate training and test sets, using only the training set to develop our baseline model. Therefore, we were unable to capture annual periodicities that could occur due to public holidays or seasonal illnesses.

We evaluated our models based on simulated failures. As a proof of concept, simple failure scenarios were introduced, consisting of a single type of error with a constant error rate. In reality, HIT failures can manifest in less predictable ways, with multiple errors co-occurring at varying error rates and durations. This could affect the detectability of the failures in the real world. Future research would need to evaluate the effectiveness of this approach using real HIT failure data and a more complex error mix.

Finally, we have focused on four types of failure. There are many other sources of errors that have not been addressed in our study. For instance, mismatch of patient identifiers caused by software errors is a commonly reported problem that cannot be detected by our approach. Furthermore, failures that impact the availability of the HIT system were not addressed in our study. These include system downtime and network availability. These failures are currently well served by existing network monitoring methods, and can also be detected by extending our approach to monitoring indices such as laboratory record creation and access time information. Finally, our study focused on monitoring quantitative fields. The detection of errors in textual clinical data has not been explored. It is likely that by using the appropriate natural language processing tools, the statistical properties of textual clinical data can be extracted. If these properties were found to be predictable (ie, in a state of statistical control), errors in textual fields can potentially be monitored using similar techniques to quantitative fields. As most clinical data are in textual form, future studies should explore the feasibility of such an approach.

CONCLUSIONS

In this study, we have applied the concept of syndromic surveillance for the detection of HIT system failures. The system has tremendous potential in the monitoring of HIT system performance, and facilitating the early detection of HIT system failures. With our increasing dependence on HIT systems, and the complexity of these systems, syndromic surveillance can provide a safety net for detecting abnormalities early, so as to minimize the harm caused by failures in HIT systems.

Acknowledgements The authors wish to thank David Rolfe, Robert Flanagan, and Ed Tinker for providing access to the data.
Contributors  MSO developed the models, analyzed the data, and wrote the manuscript. FM and EC reviewed the model and the manuscript.

Funding  This research is supported by NHMRC program grant 568612, the NHMRC Centre for Research Excellence in E-Health, and a University of New South Wales Faculty of Medicine early career grant. The funding sources played no role in the design, conduct, or reporting of the study.

Ethics approval  Ethics approval for the study was obtained from the hospital and university committees.

Competing interests  None.

Provenance and peer review  Not commissioned; externally peer reviewed.

REFERENCES


