



Making the Grade: the eHealthRisk Report Card

Brendan Seaton

Brendan Seaton is an Educator with Brendan Seaton Productions Ltd. in North York, ON.

Why do so many eHealth projects fail? Why are we so obsessed with privacy concerns when issues of patient safety fail to register on our radar screens? Why do users so often reject eHealth systems?

For more than 25 years I have grappled with the challenges of implementing information technology in health. While there have been successes, I've witnessed more than my fair share of train wrecks. All of these train wrecks were fully predictable and preventable. I recall one project that was cancelled after four years and 35 million dollars. We knew four weeks into the project that it was in trouble.

Many projects and the more savvy health organizations have conducted Privacy Impact Assessments (PIAs) and security Threat and Risk Assessments (TRAs). Many have integrated project risk assessment into their project management methodologies. But all too often these assessments are conducted in silos by external consultants who don't understand the complexities of the user environment and have no stake in the ongoing operation. And there are gaps. Patient safety and a whole range of business risks never register on our radar screens.

Politicians, bureaucrats and health care executives are concerned about the risk of eHealth to patients, health care providers and health care organizations. They are concerned that the public gets real value for the tax

dollars spent on eHealth. What senior decision-makers lack is an integrated view of the risks associated with eHealth.

We recognized this problem when I was working at the Smart Systems for Health Agency (SSHA). The competing interests and issues in the eHealth environment are formidable. It is difficult for managers and executives to identify prioritize and keep track of the many complex and inter-related risks. Working with the Waterloo Institute for Health Informatics Research (WIHIR), SSHA developed an integrated approach to eHealth risk management. This work has evolved into the eHealthRisk Report Card.

The eHealthRisk Report Card is a management system. It integrates the risk assessment processes already in place in a health care organization, fills in the gaps and presents an integrated risk profile to senior management. The risk profile includes a plan to manage the risks identified. The Report Card then helps to track the progress of risk mitigation.

Risk is about the uncertainty of outcomes, which could be either a positive opportunity or a negative threat. It is expressed as a function of likelihood and impact. Many approaches to risk management focus exclusively on the negative threat side of the equation. The Report Card looks at both opportunities and threats and helps guide management towards achieving a balance that

Class of Risk	Grade	% of Total Grade
Achieving Desired Outcomes	B	35%
Privacy Risk	A-	10%
Security Risk	C	15%
Safety Risk	C-	10%
Project Risk	B	10%
Business Risk	D	20%
Overall Grade	C+	100%

Figure 1 – Summary Report Card

The eHealthRisk Report Card is a management system. It integrates the risk assessment processes already in place in a health care organization, fills in the gaps and presents an integrated risk profile to senior management.

works in the best interests of the patient, health care provider and organization.

The Report Card tracks six classes of risk: achieving desired outcomes (such as improved patient outcomes and increased efficiency), minimizing privacy risk, security risk, safety risk, project risk and business risk. It assigns a point-in-time grade (A+ to F), which is updated over time to reflect changes in risk posture for each of the classes. The summary report card (see figure 1) is backed by a comprehensive analysis that includes the detailed information required by those who must manage the risk.

Among the critical success factors for a risk management program is the assignment of accountability for management of the risk to a senior executive and the integration of the Report Card with other management control systems such as executive performance measurement and the Balanced Scorecard.

The Report Card is conducted in three parts. The methodology guides project managers and health care executives through the identification of risks, proposes a plan for dealing with each risk identified, and then tracks progress against the plans that have been approved by senior management. These processes are well developed for privacy and security (PIAs and TRAs). For safety, project and business risk the methodology draws from best practices in the aviation, nuclear and other high-risk industries.

While it uses standardized processes, the Report Card does not take a cookie-cutter approach to risk management. It recognizes the different threat environments and business priorities that are unique to each organization. It does so in such a way that results are comparable with other organizations and can be communicated to patients, staff, regulators, business partners and payers.

An important part in the risk management process is the determination of the risk tolerance threshold. How much risk is the organization willing to accept on behalf of its patients and other stakeholders? Risks above the risk tolerance threshold must be addressed. Risk below the threshold can be accepted but monitored to ensure that their risk level does not increase.

An organization doesn't have to eliminate every risk to achieve a good grade. The Report Card grades the organization on how well they are managing the risk. Risks can be managed in one of four ways: avoidance,

acceptance, transfer and mitigation.

To avoid risk the organization's management can decide not to undertake the project because it is too risky. Accepting the risk works for risks below the risk tolerance threshold, or where the risk is beyond the control of the organization such as a natural disaster. Transferring the risk can be accomplished by taking out insurance for financial risk. Having the patient or other party sign a consent form or agreement are other ways of transferring risk. Mitigating the risk, i.e. correcting the problem that gives rise to the risk, is usually the preferred approach.

Someone in the organization must be responsible for tracking the risks and ensuring that the management strategies are implemented. The Report Card should be updated over time so that management can see where grades are improving or slipping.

Risk is a good thing. If we wanted to avoid all risk we would stay in bed all day. As in our daily lives, risk management allows us to get up, go outside and enjoy the day. The risks are still there, but we know about them and are prepared to deal with them. The eHealthRisk Report Card is a methodology that will allow CEOs, CIOs and health care providers to go about their day knowing that their eHealth systems will be there and will be working when they are needed. ●

Brendan Seaton is one of Canada's leading authorities on the management of eHealth risk. He acknowledges the contributions and groundbreaking work of Gary Young, Rupak Mazumdar and Gila Pyke of the Risk Management Team at the Ontario Smart Systems for Health Agency and Dominic Covvey, Founding Director of the Waterloo Institute for Health Informatics Research.

Brendan and the WIHIR will be offering one-day intensive workshops on the eHealth Risk Report Card, Privacy and Security on the campus of the University of Waterloo.

Follow eHealth risk issues on Brendan's eHealth risk blog at www.ehealthrisk.blogspot.com.