Privacy Lessons Learned from an Operational Health Information Exchange

Governments and care providers across the globe are investing in health information exchanges (HIEs) and electronic health records (EHRs) without fully understanding the privacy implications of broad-scale electronic access to protected patient information. Lessons learned from NHS Scotland's fully operational HIE deployment[1] could save the healthcare industry time, money and reputation.

A FairWarning® White Paper

Trust but Verify®

Introduction

In the recent years there has been a drive in Europe, Canada, Asia Pacific and the United States towards an integrated Electronic Healthcare Record (EHR) at the care provider level as well as toward Health Information Exchanges (HIEs) which facilitate the electronic exchange of patient information between care providers at a provincial, state, regional or national level.

The benefits of EHRs and HIEs have been widely discussed and detailed in clinical literature. However, this paper will consider the actual and unique privacy challenges in designing and managing a fully operational EHR and HIE. Through real-world Privacy Use Cases, this white paper offers insights into the misuse of broad-scale access to patient information within a given care provider as well as brand-new privacy vulnerabilities resulting from patient information access across care provider boundaries.

Further, this paper offers specific business and technology considerations for the use of proactive privacy auditing applied to both EHRs and HIEs enabling healthcare providers and health information exchanges to confidently connect physicians, clinics, patients and affiliates.

---

[1] Scotland's Emergency Care Summary Is a First Step Toward a National Health Information Exchange.   Gartner G00149175 June 2007

About FairWarning®

FairWarning® is a global leader in appliance-based software solutions which monitor and protect patient privacy in electronic health records enabling healthcare providers and health information exchanges to confidently connect physicians, clinics, patients and affiliates. FairWarning®'s turn-key privacy auditing solutions are compatible with healthcare applications from every major vendor.

Notices

FairWarning, Inc.
Email: Solutions@FairWarningAudit.com
Web: www.FairWarningAudit.com
Phone: U.S. 727 576 6700, U.K. 0-800-047-0933

Background

NHS Scotland serves the health needs of Scotland's 5.2 million citizen-patients who live spread over 32,000 square miles in the northern United Kingdom mainland and surrounding islands. NHS Scotland operates 14 Health Boards[2] (HBs) across the country and is comprised of 132,000 employees, 8,500 physicians and 7,000 contracted healthcare practitioners.   Well ahead of its time, in 2003 NHS Scotland recognized that an operational, country-wide HIE could produce fiscal efficiencies and deliver care providers better and more consistent patient information. By 2006, Scotland's Emergency Care Summary (ECS) system was rolled out country-wide. In 2007 Gartner[1] documented ECS as a successful implementation of an HIE sensibly delivering patient care value.

NHS Scotland's Emergency Care Summary has now been in operation for five years and offers lessons on privacy and security considerations that are unforeseen without the benefit of a fully operational HIE. In December 2010, NHS Scotland also began the implementation of a standardised EHR following a successful implementation in the South East of Scotland.

The NHS Scotland Health Information Exchange

The main HIE is the **Emergency Care Summary** (ECS)[3]. This record initially comprised demographic, prescribing data, and allergies for 99% of the Scottish population, approximately 5 million people, and has very defined access and audit rules. It is updated twice daily from the family doctors' clinical systems, and was initially intended for use in emergency situations where the patient was conscious and could provide consent for access. Although ECS is managed in a National Cloud Data Centre, each Health Board manages and has responsibility for the access of its own staff and every access must be reviewed monthly.

NHS Lothian, where the author was based, had 2000 staff with authorized access to Emergency Care Summary. In an average month, there would be 15,000 accesses to NHS Lothian's patients, mainly by internal staff, but also by staff from other HBs. Each access to a patient's record had to be checked and followed up to ensure privacy protocols were not being abused, this task required two staff members to dedicate one week every month.
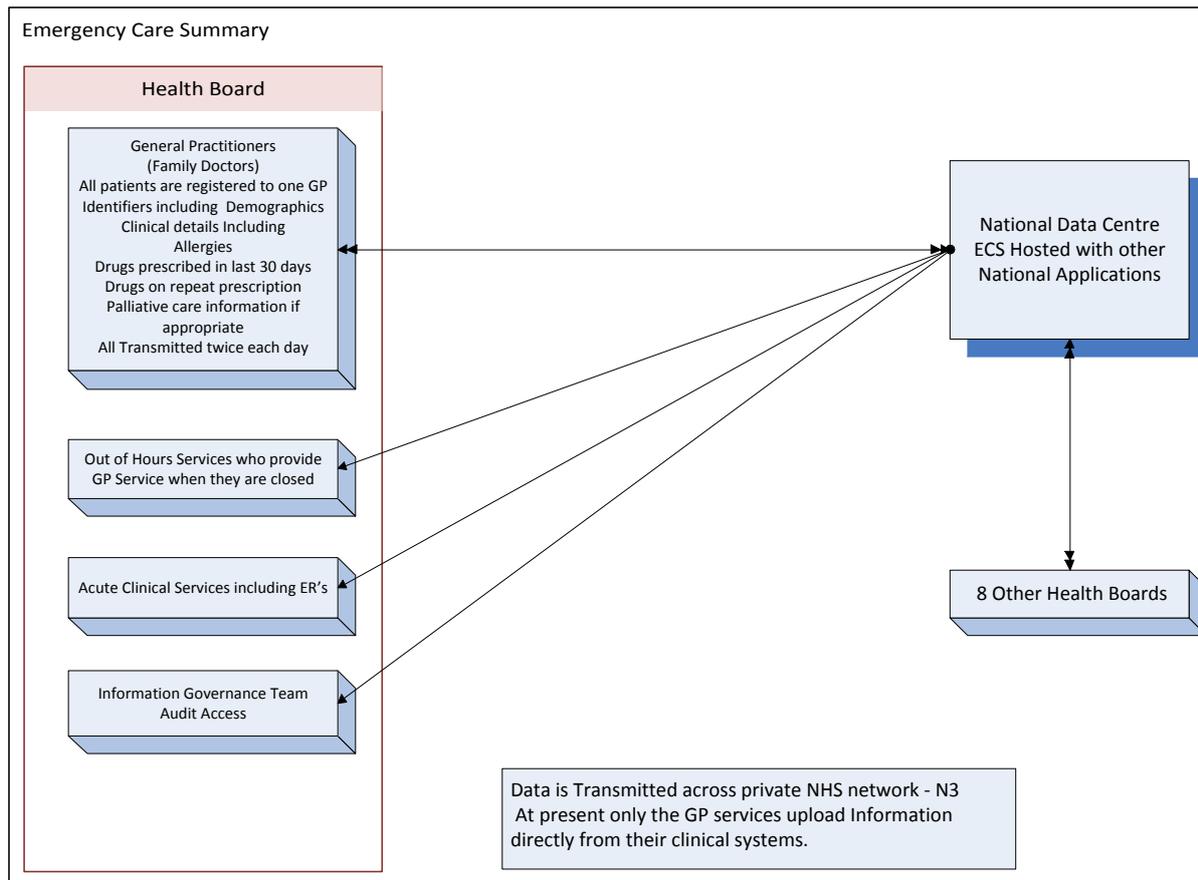
---

[2] Scotland is divided up into Health Boards which are 13 territorial covering a geographic area and 9 "Special Health Boards" covering specific National organizations.

Figure 1. Emergency Care Summary as Primary HIE Application

There are two broad categories of privacy considerations:

1. Those related to access of patient information through the HIE across HB boundaries and
2. Those related to broad-scale access to an EHR by employees and contractors within a Board.

The ECS application divided its users into two main role groups, Clinical and Administrative. Clinical groups could see all data, while Administrative groups were only able to see demographic data. As the inhabitants of Scotland are each registered with Family Doctors, these practices can only see their own practice patients. However, clinicians in Acute Care hospitals and ERs have the ability to see all patients. Each time a patient's clinical or demographic details are accessed anywhere in Scotland, their Family Doctor's practice receives an indicator that access has occurred. They will not know who made it, their location or whether the access was legitimate, only that an access has occurred.

It was noticed in an adjacent Health Board that a number of unusual accesses to patients in the ECS through the HIE were occurring and that the pattern was suspicious. After an investigation, which took over four weeks, it was found that a Hospital Consultant (Attending) Physician was systematically searching through the records of a number of politicians, TV personalities and sports personalities. He was looking at the drugs prescribed in order to determine whether they were suffering from chronic complaints.

- This was a clear abuse of access. It was discovered both at the Consultant's HB as well as at the HB where a TV personality lived, when they were unable to get supporting documentation from the HB where the user (Consultant) was based
- The Consultant was suspended and reported to the General Medical Council for disciplinary action.
- It was observed that detection of this HIE access abuse was uncovered by unreliable manual processes and that investigation of a single incident required weeks of investigation

Privacy Use Case 2

A junior doctor was noticed to have been searching the ECS for female patients within an adjacent HB area. As it turned out, an unconscious female patient had been brought into the ER by a recent acquaintance who knew only her first name, date of birth, and town of residence. The doctor was only searching based on first name and date of birth, and stopped searching once he found an address match. Using this search, he was able to confirm that the patient was an insulin-dependent diabetic. Fortunately, towns in that area are small and he hit the correct person on his 9th record.

- Although this was a clear breach of the access protocols, it was accepted by the local HB that it was for a justifiable clinical reason and no further action was required
- It was observed that auditing of the HIE ensured the physician was able to conduct their responsibilities in privacy and was <u>cleared of any suspicion</u>

The Electronic Health Record

Today NHS Lothian operates ***Intersystems Trak HealthCare[4],*** a combination of Patient Management System and full EHR. The NHS Lothian implementation of this EHR started in 2004.

From its inception and early development, it was designed to hold details of Antenatal appointments, clinic attendances, inpatient services including bed management and infection control. It enabled the ordering of radiology and laboratory tests, as well as displayed results including autopsy. It is truly beyond 'Cradle to the Grave'. It connects Acute and Community health services in four major hospitals with 2500 inpatient beds including a children's

---

[4] www.intersystems.com/**trak**care/index.html

hospital, two Emergency Rooms (one of which is the busiest in the UK), and some 150 clinical sites within the community. It links to a number of other clinical systems, including allowing for viewing PACS images taken at any NHS Lothian site.

Currently, it is in use by more than 23,000 staff daily with up to 14,000 concurrent users and at last count provided the EHR for approximately 1.25 million patients. It does not at present cover mental health services.

Practical Limitations Drive Need for Privacy Auditing

Role-based access controls are often used to segregate and manage access to both HIEs and EHRs. While they provide a level of protection they are not a complete solution on their own, but merely another layer of privacy protection. Although the ECS through its basic design and limited functionality is capable of role based access controls, the EHR had and continues to have major problem over user access. With a need for the EHR to be accessed 24/7/365 in any of nearly 200 locations by a variety of clinical, clerical or administrative staff, other issues came to the forefront.

Although access controls can be setup allowing only clinical staff to view the clinical elements of the EHR, there are many clerical staff who also require that level of access for legitimate reasons. As financial pressure increases in health, as in other areas, clerical roles particularly overlap requiring care in the selection of the work flows and data that are accessible. While staff may be given read-only access to the clinical record, even this limited access may be sufficient to initiate a breach of privacy.

Further challenges arise where clerical and nursing staff have two or more part time roles requiring different levels of access. The mobility and nature of shift patterns often preclude locations from being used effectively in limiting access unless there is a large back office function available on a 24/7 basis. An element of trust to use correct level of privilege is then passed to these staff members.

The EHR is an active element in the patient's diagnosis and treatment, as it is used to order laboratory and radiology investigations with the primary clinical groups as well as the main acute locations able to access results. For example, patient records needed to be passed to the correct radiology department, rather than another location nearby. This was necessary due to restrictions not in the EHR but a function of the five PACS systems in use.

Many outsiders believe that a "break-the-glass" function can be used to view certain elements of the record. However, it turned out that there were insufficient glaziers available to confirm that the break in was legitimate and replace the glass.

Experiences and Lessons Learned which Necessitated Privacy Auditing

During the early deployment of the EHR, when its access was limited to clerical and administrative staff, it became clear that audit of access would be an increasing requirement of its acceptance by the public. It was also realised that auditing access to the EHR alone was increasingly demanding across the organization, and at that stage the EHR was only available to 50% of its planned user base.

As more clinical information became available within the EHR it became a target for curiosity.

Privacy Use Case 3

It was announced on local radio and TV stations that a high profile prisoner in a local jail had been assaulted and admitted to one of the major hospitals. Within minutes of the announcements, the admitting ward started to notice temporary lock ups in that patient's EHR. The security and privacy staff were asked to monitor access to the EHR. As this was a manual process, it was necessary to print out audit reports and then take these to the attending clinician to validate who was legitimately accessing the EHR. This time-consuming process involved a very busy clinician and it was apparent that there was a serious privacy issue which required further investigation.

- 31 staff members were disciplined, up to and including dismissal, for accessing the prisoner's record inappropriately over a 3 day period
- Staff were re-trained on privacy regulations and confidentiality requirements
- It was discovered that manual privacy auditing processes, even in a specific area and against a specific patient, was immensely labour-intensive

Privacy Use Case 4

A patient access request under the Data Protection Act was made by a member of staff as to who had viewed her EHR including clinical elements. After the birth of her child, family members had made comments based on information that could only have come from the EHR regarding her previous clinical history, and she believed a colleague had access and shared this information.

Upon review, it was found that her colleague had not accessed the record. However, shortly after she announced that she was pregnant, her father had accessed the record. The details viewed included basic information on a termination that had taken place 2 years previously and had been unknown to the family.

- This was a clear breach of her privacy and confidentiality by her father who worked elsewhere in the organisation and who had legitimate access to the EHR. It was also a breach of his contract of employment.

- The father left the organisation and no further legal action was taken as it would have caused even more issues within the family

As more people became aware of the ability to search audit trails within the EHR, there was a substantial increase in the number of staff requesting information on who had viewed their record. This increased the pressure on the team responsible for providing the reports, who were being kept from their regular duties by the extra requests. A three week backlog of investigations became normal, and was increasing

Privacy Use Case 5

A terminally ill patient was admitted through the ER for an unrelated complaint. The ER staff was unable to order investigations for this patient, as the record was being continuously locked by a member of the administrative staff in another location. Upon investigation, it was discovered that the administrative staff member was the patient's neighbour's daughter. Each time the patient was admitted, the neighbor was calling her daughter for clinical details. The mother in turn used the information to discuss the case with other friends, none of whom had any clinical background.

- The in-depth investigation on this event uncovered that this breach had been ongoing for some months.
- The staff member had viewed a number of clinical reports before the physicians responsible for the case
- Although the staff member initially denied accessing the record, when confronted with the evidence accrued over several days of work on the audit trails of the EHR, she resigned immediately and left the NHS
- This case indicated that there was a serious clinical risk where inappropriate access could prevent ordering and viewing of urgent investigations and results

After Case 5, a pilot of manual proactive auditing of the EHR revealed that providing coverage of each clinic and ward on a random basis would require 4 staff and take 3 years to ensure coverage of all clinical locations!

Concerns grew as anecdotal evidence suggested staff members were abusing EHR access, looking up colleagues', friends' and neighbours' records. Evidence from the small number of reactive audits confirmed that this was occurring.

The root cause of all the privacy breaches was an abuse of correctly granted access rights.

There was an assumption by some staff that because the record was available it was permissible to view. It was necessary to remind staff of the existing policies around access and that disciplinary action would be taken against those involved in breaches.

Discussions were also sparked over the potential of sharing data from the EHR, ECS (HIE) and several specialist applications across a much wider geographic area and user base through a Clinical Portal. In addition, it was known that there was to be an increase in the

user base of the ECS within the Acute setting to improve patient safety with respect to drug regimens on admission, which meant even greater patient privacy vulnerabilities.

If the public's confidence in NHS Scotland's and NHS Lothian's ability to provide privacy within the EHR and HIEs was lost, the HB, which had made a substantial financial investment in electronic systems to benefit the patient, might be forced to make major changes to its strategy and in doing so, lose many of the clinical benefits accrued by the EHR and HIE.

A process permitting proactive audit of access was required if patient confidence was to be maintained. It was also essential that the process be as automated as possible, to minimize demand on very limited resources.

Many products on the market could audit access to the network at log on level, whilst others could measure the log on attempts to applications. However, only FairWarning® appeared to provide the granularity to address and read the application audit trails. After discussions and some negotiation with FairWarning®, the solution was procured.

Since none of NHS Lothian's applications were on the list of systems previously covered, NHS Lothian was concerned as to how long it might take to produce results. However, three weeks after completing installation, the application was ready to run.

The first report was against one of our National applications, Scottish Care Initiative (SCI) Store, which is a repository for results which fed a number of local and other national systems including results of investigations requested by family doctors on their patients and the results of all investigations from laboratory services. It was managed locally and its workflows were well understood by the local team. FairWarning® was also fed information from the HR system to provide details including staff groups, working location, and personal addresses.

Fears were confirmed: staff were using SCI Store to look up their own, family member and colleagues' results, all of which were against local policies, professional society guidance and in some cases the law.

Over the next few weeks TRAK and ECS were added to SCI Store. An NHS Lothian team brief item reminding staff of their responsibilities with regard to confidentiality was circulated. The number of staff breaching the rules dropped by 75%, the message was being received.

Over the next few months gentle reminders were required to keep the numbers low. After a year a further strongly worded letter was sent to every member of staff reminding them of their legal and contractual position with regard to patient privacy. The numbers continued to fall to a trickle.
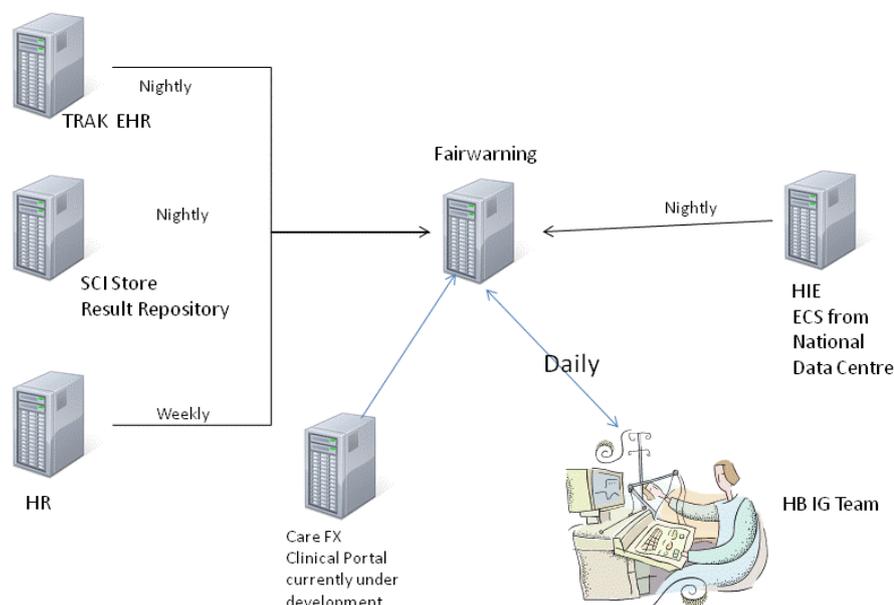
Fairwarning Audit Typical Scottish Installation

Figure 2. Typical FairWarning® Install for an NHS Board Interacting with the National HIE

Benefits Achieved through Automated EHR and HIE Privacy Auditing

Using FairWarning® privacy breach analytics, a number of simple dashboard reports were created against the application's audit trails and linked to the HR system. These were scheduled to be automatically presented to the Information Governance team each morning providing information on:

- Self snooping
- Reading family records
- Viewing colleagues records
- Viewing neighbours' records
- Excessive number of records being viewed in a given timescale by one user

These can be read against single or multiple applications.

Privacy Use Case 6

After FairWarning® had been running for about 6 months, a very high profile patient with complex needs was admitted in similar circumstances to the patient in Case 3. An alert was placed against the patient records on the EHR/HIE and the other applications covered by FairWarning®.

The number of staff found to be abusing their access and viewing this patient's record through curiosity or any other unauthorised purpose was only 3 in the first 3 weeks, a great improvement over previous high-profile patients.

Message was getting across!

Benefits of Privacy Monitoring Software

Patient

The patient could within minutes of a request be given a list of everyone who had viewed their record in the EHR or any of the HIEs in use. Some past relationships and distant cousins come to light for all the wrong reasons.

Password Sharing

A simple report was created which could warn when an EHR user account was being used in more than one physical location simultaneously or within a timespan in which it would have been impossible for the user to move to that location. This was in breach of the Security Policy and staff were subject to final warning followed by disciplinary action.

Investigations

Previously, when a member of staff was suspected of viewing another's record it could take several days to go through the application audit trails of access and activity. Now, a report showing an individual user's access across the clinical applications and patient records involved can be set up and run in moments. This reduced the turn around time on such requests from over 10 working days to less than 15 minutes. As a result, staff were not being kept unnecessarily in suspense awaiting the outcome of investigations.

Where disciplinary action was required after a breach of privacy the HR and legal team could be given the evidence almost immediately and meeting with line management arranged the same day as the breach had been discovered.

The HIE monthly audit of access took between three and four days prior to the introduction of Fairwarning® who created a bespoke report.   This reduced the audit time to 45 minutes! Additionally NHS Lothian worked with FairWarning® and the National developers for ECS and Intersystems on another report which provided exception to the national audit policy. It alerted us if the ECS was used to look at patient information within the acute setting and the patient did not have an attendance within 48 hours of that query. This permitted us to roll out access to the HIE much more widely than envisaged, improving patient safety through precise correlation of drugs the patient had been prescribed by their family doctor.

For NHS Scotland and its Health Boards like NHS Lothian, the use of proactive privacy auditing by FairWarning® applied to both EHRs and its HIE is enabling confident connection of physicians, clinics, patients and affiliates resulting in more consistent and effective care for patients and a fiscally responsible approach to delivering care.

The Future

The culture at NHS Lothian is being changed, with staff becoming increasingly aware of the need to provide and respect patient privacy at every level!

In late 2009, InterSystems TRAK Healthcare was appointed to provide the EHR to all Health Boards in Scotland.

In early 2011, after a successful pilot, CareFX received the contract to provide a clinical portal taking key information from the HIE and EHRs across HB boundaries.

In March 2011 FairWarning® received the contract to provide privacy monitoring software to every Health Board in Scotland.

Scotland will soon have an HIE which will cover a common EHR, capable of exchanging data on 5 million patients and providing them with a higher assurance of privacy than many other countries.

About the Author

Ted Boyle joined the NHS in 1996 after a successful career in the Royal Air Force. In 2001, he became responsible for the team of staff managing a Patient Administration System covering two of the United Kingdom's larger teaching Hospitals. During the next 10 years this system was updated to form a full Electronic Health Record. As a qualified Data Protection and IT Security Officer, Ted's responsibilities were widened to include all Information Governance issues arising from the use of EHRs and HIEs. In all, the EHR holding 1.25 million records is used by 23,000 staff, in 4 major Hospitals, including the busiest ER in UK and 150 other locations across the South East of Scotland. He was also responsible for the audit of access to all the clinical applications as well as the security of the infrastructure which hosted the application. Ted now has his own consultancy specialising in Information Governance in the health arena.