

Privacy Lessons Learned from an Operational Health Information Exchange

*A conversation on lessons in
broad-scale access to protected
health information*

[View the full replay](#)

FAIRWARNING®

Trust but verify®



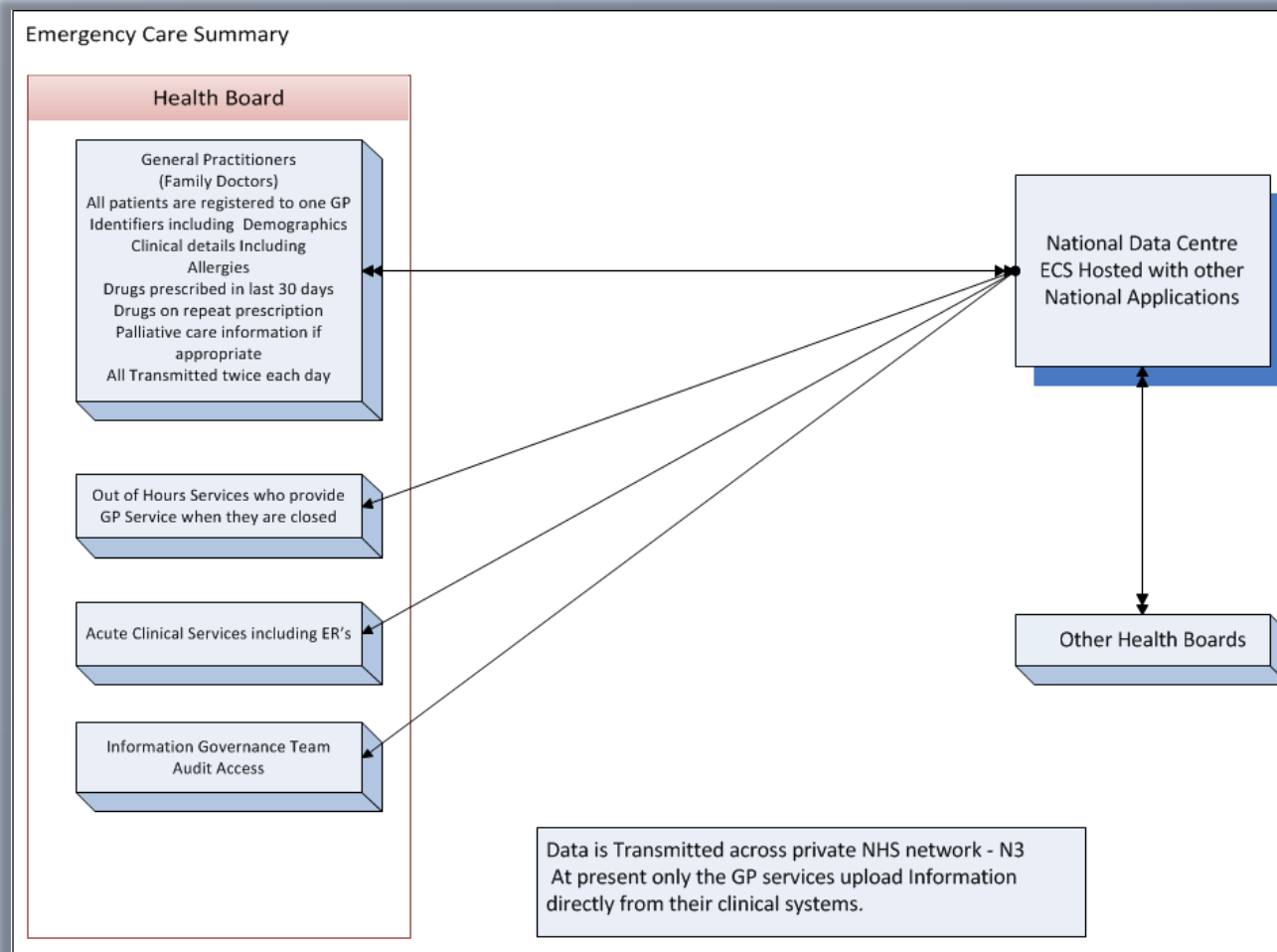
NHS Scotland Overview

- 5.2 Million patient citizens
- 32,000 square miles in Northern United Kingdom
- 14 “Boards” comprised of 132,000 employees
- 8,500 physicians and 7,000 contracted practitioners

NHS Scotland Health Information Exchange – Emergency Care Summary

- Conceived in 2003
- Country-wide rollout completed 2006
- 2007 documented by Gartner as “sensible” HIE
- Initially demographic, prescribing & allergies data for five million people, 99% of citizens
- ECS Managed in National Data Cloud Centre, each Health Board manages access of its staff, access reviewed monthly

Emergency Care Summary



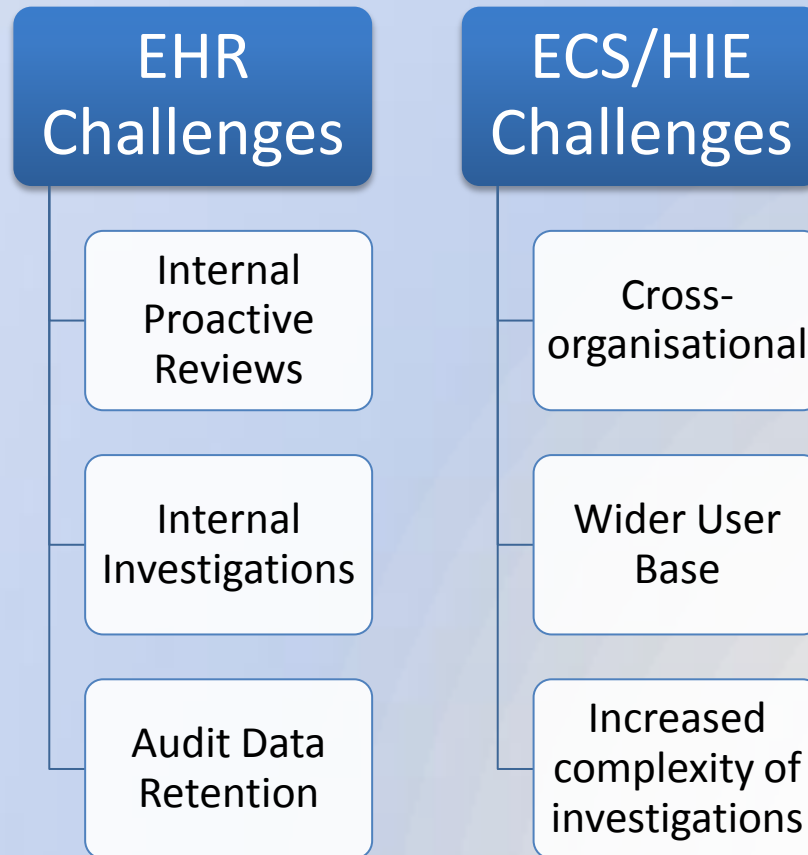
ECS Access Review at the Health Board Level

- NHS Lothian had 2000 staff with authorized HIE access
- Average of 15,000 monthly accesses to NHS Lothian patients
- Access mainly by internal staff but also by other Health Boards
- Each access reviewed

NHS Lothian

- Located in Edinburgh, Scotland
- 23,000 staff
- InterSystems Trak Healthcare PMS and full EHR
- 24/7/365 EHR access from 200 locations for 1.25 MM patients
- Access controls a challenge to maintain
- Even read-only access presented privacy breach opportunities

Privacy Challenges of Broad-Scale Access of Electronic Patient Information



EHR Privacy Use Cases

- # 1 Reactive investigation
 - *VIP / Tobyn*
 - *Neighbour*
 - *Staff*
- # 2 Pro Active Audit / Alerts
 - Limited coverage base on manual process
 - 4 staff, three wards or clinics week = 3Yrs

HIE Privacy Use Cases

- # 1 Reactive investigation
 - *VIP*
 - *Unconscious patient*
- # 2 Pro Active Audit
 - 15,000 entries per month
 - 4 staff, 1 week per month
 - On-going national requirement for review

Audit Tool Requirements

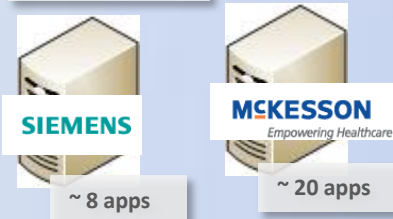
- Proactive - close to real time if possible
- Automate discovery process
- Manage more than one application simultaneously
- Measure Application Internal work flows
- Minimise false positives
- Link to HR systems if possible
- Needs to deter:
 - Self snooping, Colleagues, Neighbours, “VIPs”
- User Friendly

Turn-key auditing support for over 125+ EHRs and applications

Major Suite Vendors



~ 5 apps



Other suites and supporting applications

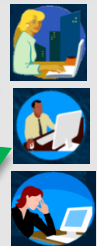


New or in-house apps added in 1 day

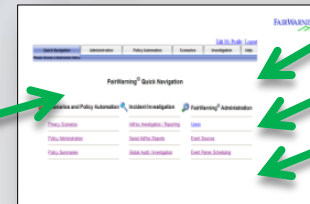
User information from business & identity applications



FairWarning® Users



Privacy analysis, alerting, reporting

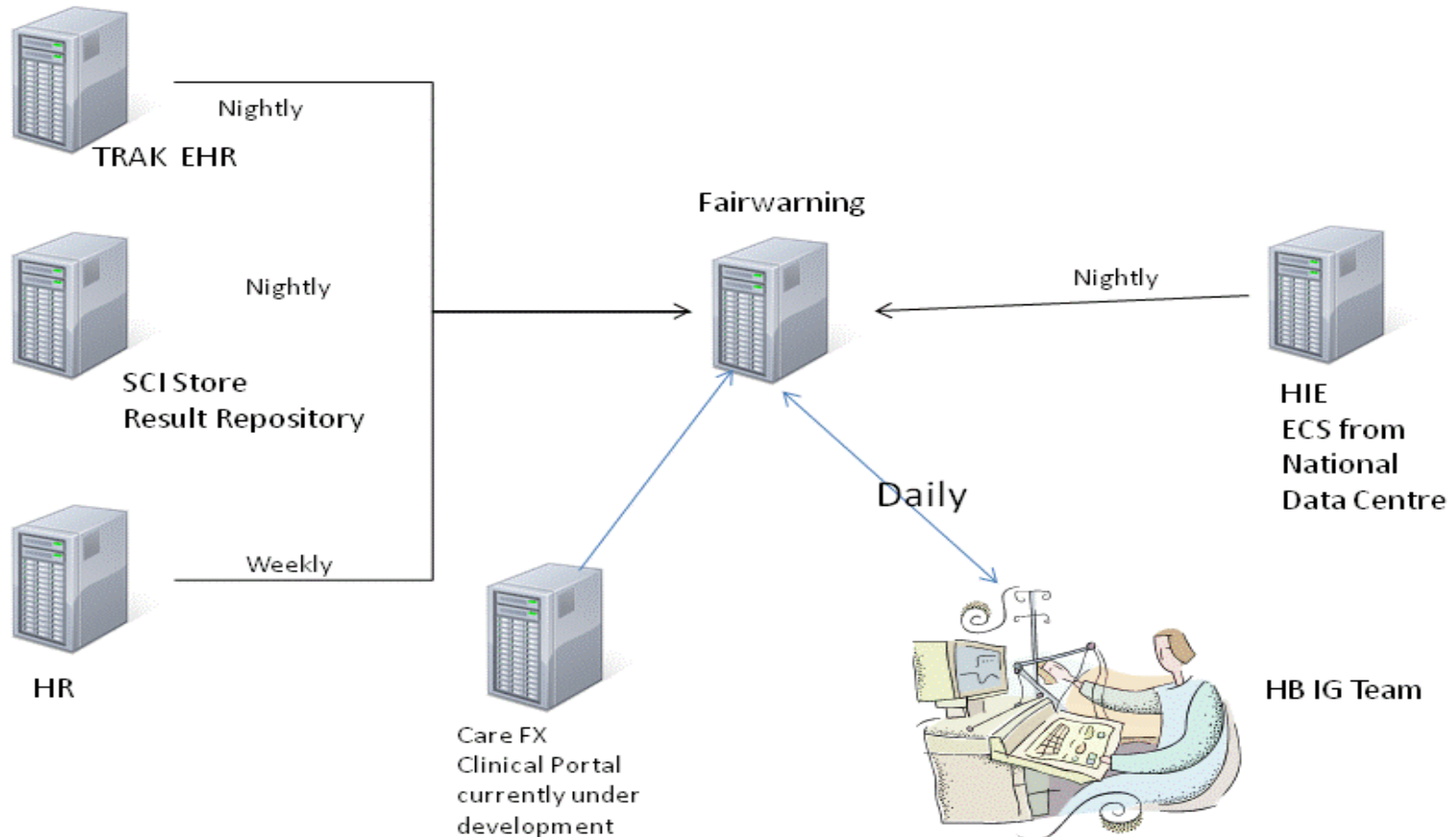


Patient privacy incidents Detected by FairWarning® optionally sent to SIEM

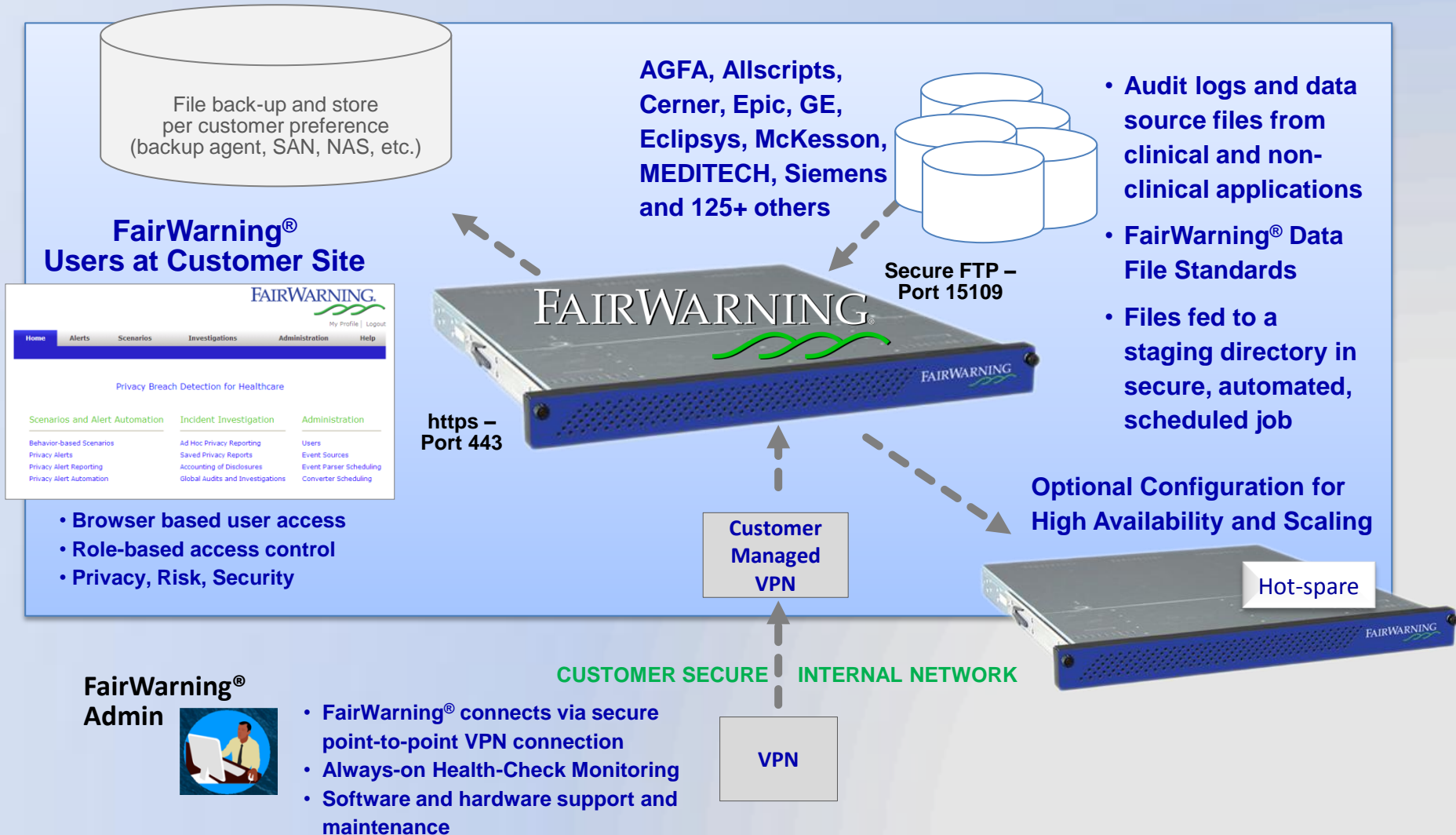


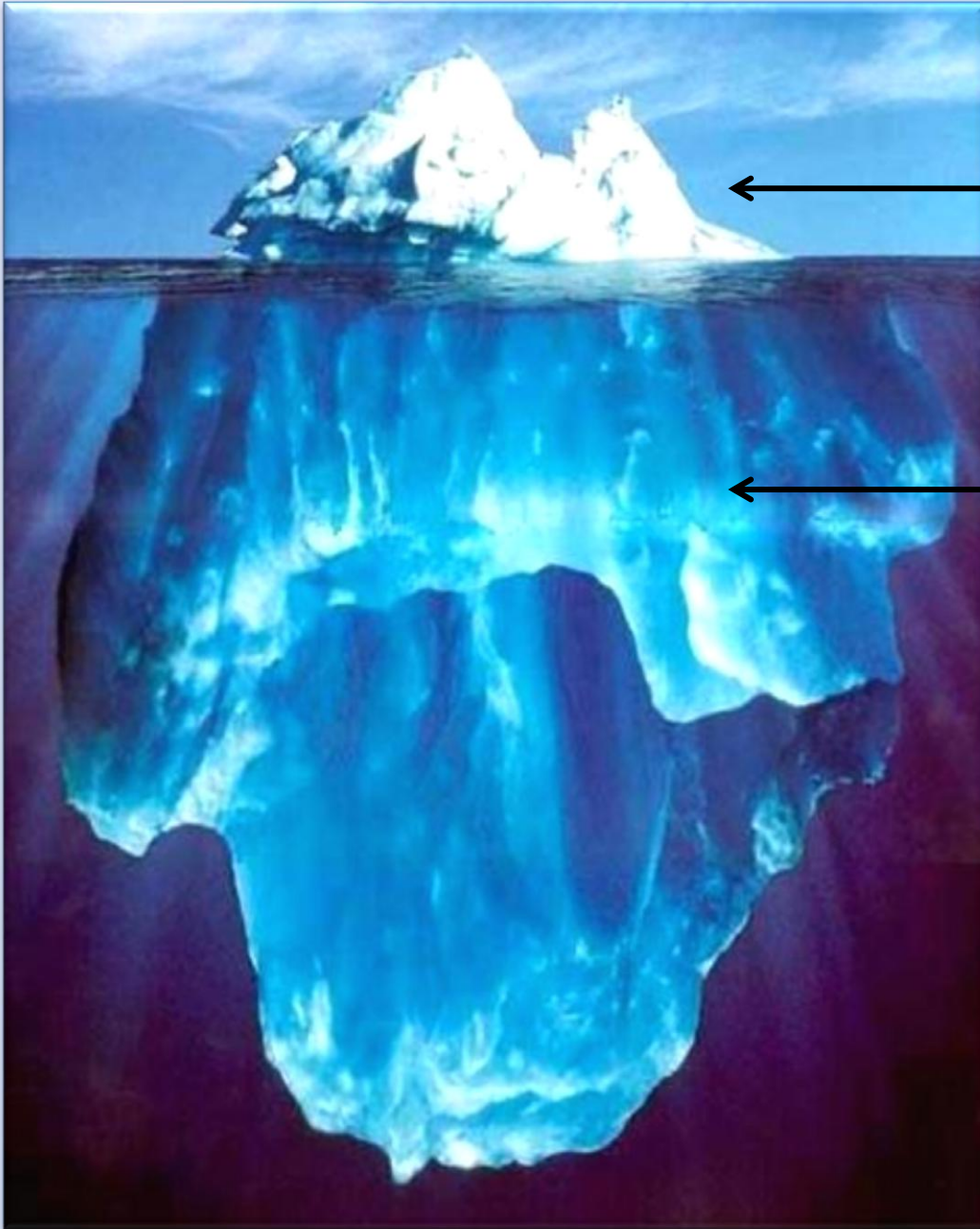
Deployment

Fairwarning Audit Typical Scottish Installation



Network and System Architecture

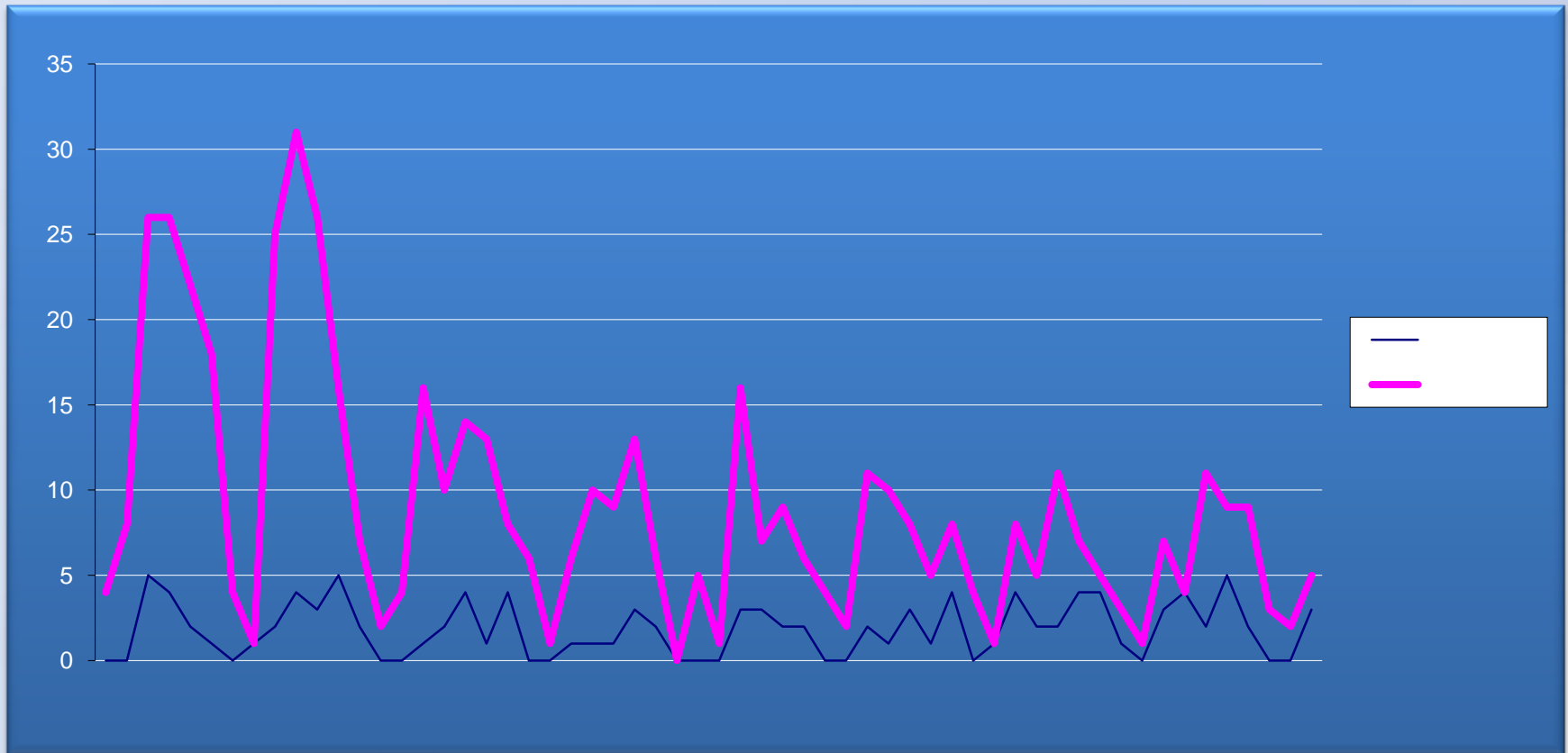




What you find.

What was found.

What was found



Benefits of a FairWarning Deployment

- Self Snooping
- Reading Family records
- Viewing colleagues records
- Viewing Neighbours records
- Excessive number of records being viewed in a given timescale by one user
- Alerts
- Patient Benefit
- Password Sharing
- Investigations

NHS Scotland Privacy Goals

- Leverage EHR and HIE investments to serve growing healthcare needs of Scotland's citizen-patients
- Uninterrupted growth and use of electronic health records and Emergency Care Summary (ECS/HIE)
- Create a culture of privacy at care providers across the country of Scotland
- Country-wide, consistent treatment of patient privacy

NHS Scotland Privacy Initiative

- National Contract
- All Health Boards
- National Clinical Applications
- 22,000 Beds, 40 Major Hospitals
- 110,000 users
- New Clinical Portals

NHS Scotland Country-Wide Privacy Auditing

- National Contract
- All Health Boards
- National Clinical Applications
- 22,000 Beds, 40 Major Hospitals
- 110,000 users
- New Clinical Portals

Considerations

- Policies in place
- Communications plans
- Reminders
- Disciplinary process agreed
- Same for all?
- Transparency over investigations

Privacy monitoring as an Foundation for EHR and HIE privacy and security

- Privacy monitoring life-cycle integration points:
 - *Authoritative user store, filtering and analytics (identity)*
 - *SIEM*
 - *Storage & data management*
 - *Compliance management*

EU Regulatory Framework

- EU Directive 94/46/EC
 - European Data Protection Supervisor
- Data Protection Act 1998
 - Information Commissioner UK
- ISO/IEC 27000-series Security Standards
- Professional Guidance
 - General Medical Council, Nursing and Midwifery Council
- Local Employment Contracts

U.S. Regulatory Framework

- **HIPAA Security Rule (2003 / 2005):**
 - **§ 164.308 (a)(1)(ii)(D) Information system activity review.** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
 - **§ 164.312(b) Technical safeguards.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
- **ARRA HITECH Privacy (2009):**
 - Definition of privacy breach
 - Willful neglect
 - Patient disclosure
 - Governmental notification required
 - Media Notification (500 or more)
 - Increased fines and precedent
 - Ability of state attorney general offices to bring lawsuits against care providers
 - Increased systemic audits
- **Meaningful Use Criteria (2010):** Level 1 certification requires an EHR to produce an audit log HITECH 45 CFR 170.302(r). Conduct a security risk analysis per HIPAA 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies...
- **Proposed Accounting of Disclosure Rule (2011):** Under the May 27th, 2011 proposed accounting of disclosure rule care providers will be responsible for providing access reports for disclosures of information even for treatment, payment and healthcare operations. Providers, plans and their business associates will be required to maintain for 3 years the information required to produce the reports. The rule is available for public comment in the Federal Register through July 2011

Planning for success

- Buy-in from Executive Stakeholders
- All stakeholders involved in kickoff and periodic updates
- Communicate “why we are deploying privacy breach detection”
- Empowered project management with access to expert data source resources
- Phased approach to deployment of audit sources and analytics
- Prioritize analytics to achieve “first success”
- *On-going* training of multiple personnel important to lasting success
- Investigation, remediation, sanctions, and training are essential

“Gotchas”

- “Trying out” a range of analytics rather than prioritizing
- Lack of remediation, sanctions, organizational buy-in and work-flows – a Privacy Breach Detection deployment will not fix a broken process, it will only reveal a broken process
- Plan data retention strategy up-front, it can be a “phased approach”, but it needs to be planned and a priority
- Low-grade technology that fails to keep pace with growing demands – look for KLAS rankings, www.klasresearch.com

Technology risks to the business case

“Weakest link breaks the chain”

- Comprehensive and centralized EHR audit log management across all sources of volume
- Proven-in-production, turn-key support for broad range of EHRs and healthcare applications
- Ability to add new audit sources rapidly and affordably
- Context-aware analytics that combines audit logs, user data and patient data
- Support for authoritative user data for filtering false-positives (Lawson, PeopleSoft, identity)
- Extreme scalability with seamless path to high availability
- Zero FTE impact for network & systems operations
- Proven speed-to-value supported by technology and well documented deployment methodology
- Health-check monitoring of hardware, systems and supporting data processes
- Clear path to real-time support

Questions?

FAIRWARNING[®]

Trust but verify[®]



Information Assurance

- Patient Identity
- Staff awareness and training
- Alignment of Expectations
- Data Corrections
- Access Controls

Today

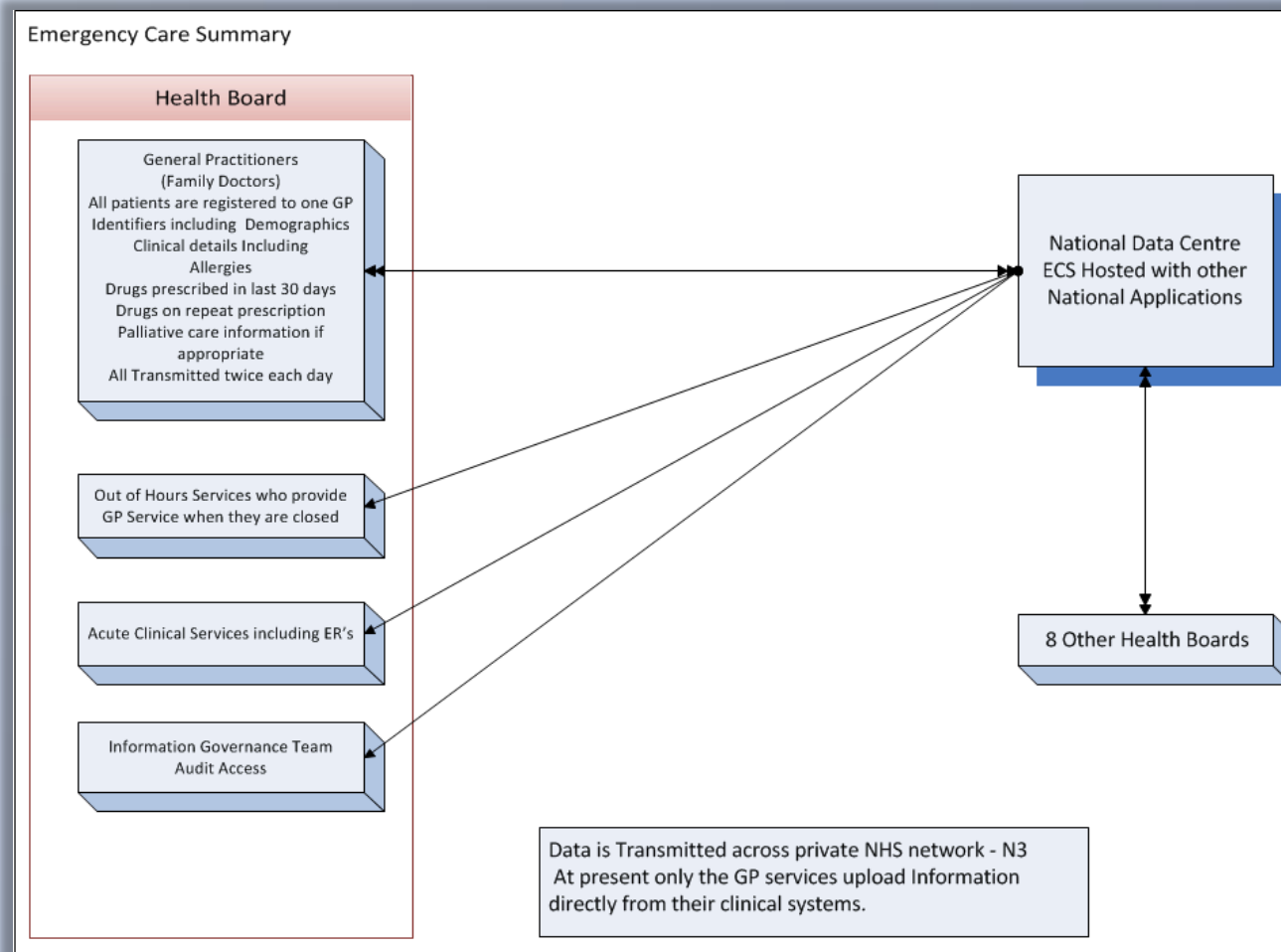
- The NHS in Scotland
 - The Regulations
 - The Applications
- Security
- Privacy Auditing needs
- A Solution

The National Health Service in Scotland

“Care is free to all at the point of delivery”

- Health is a “devolved” matter funded by Scottish Parliament
- 12 Geographic Health Boards
 - Clinical services
- eHealth Applications
 - Local and Nationally ‘Cloud’ Data Centre

Emergency Care Summary



InterSystems TRAK Healthcare

- Patient Management System Lothian 2004
 - Now being rolled out nationally
- Emergency Rooms x 3 one which is largest in UK
- Inpatients in 4 Acute hospitals 2500 beds
- Outpatients –150 sites
- Maternity
- Radiology
- Laboratory
- Community Nursing and other health professionals
- 23000 users with up to 12,000 concurrent user in Lothian

Baseline Security and Disaster Recovery Experiences

- *Hardware Restore*
- *OS Patching*
- *Network*
- *Desktop and mobile devices*

State-of-the-art security still leaves patient privacy gaps