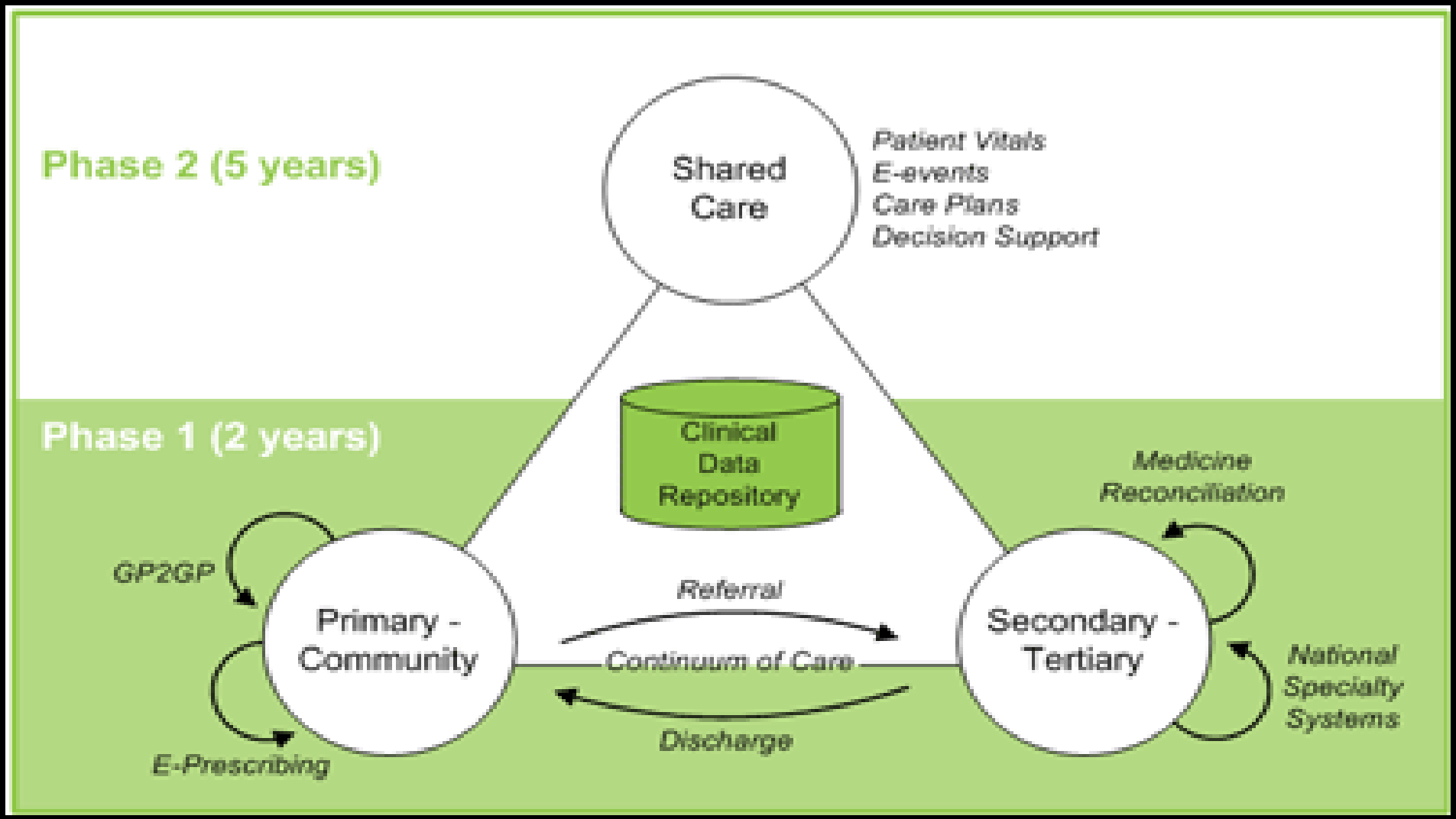
Repositories of Personal Health Information

Ross Boswell

Clinical Director of IT

Counties Manukau DHB

NZ National Health IT Board Vision



Issues with Repositories

Breadth

The increasing breadth of information being collected and held

Privacy vs Accessibility

Striking a balance between accessibility of health information and the preservation of privacy

Issues with Repositories

Consent

Arrangements for the use and disclosure of personal information when the patient's immediate and current consent cannot be obtained

Patient Access

Issues for individuals accessing their own health information, or the information of relatives or associates

Issues with Repositories

Governance

The governance of information held collectively

Non-Direct-Care Usage

The associated uses of information: teaching, research, quality improvement, and funding

Increasing Breadth of Information

The Auckland regional (*TestSafe*) repository started with laboratory reports. It has extended to:

Current	Future
Laboratory	Clinic letters
Radiology	Discharge summaries
Cardiology	Clinical referrals
Metrics	Immunisations
Respiratory	Implants
Dietetic	Allergies and
Dispensing	Adverse reactions

Privacy vs Accessibility

Prospective or Retrospective control?

- Role-based access
- Audit trail
  - Patient-centred audit
  - “Fingerprint” audit

Emergency access

Consent

“Patient not present”:

- Laboratory tests
- Referral
- Consultation

Patient Access

“Duty of care”: understanding and explanation

Duress?

Permission for proxy access

Workstation security

Non-Direct-Care Usage

Teaching

Audit

Research

Quality improvement

Funding

Information Governance

- Who “owns” the information
- Who can access it?
- Who determines access:
  - Data guardians?
  - Ethics committee?
- Public good vs private good

TestSafe
Auckland Regional Repository

- Lab reports from hospital and community labs
- Radiology reports from hospitals
- Cardiology (ECG, Echo), Respiratory, Endoscopy and other reports
- Community pharmacy dispensing reports
- Clinical documents (EDSs, outpatient letters)
- Opt-off privacy model: 1.1 million patients, 96 have opted off

TestSafe: What Works Well

- Opt-off privacy model
- Open access audit trail
- Clearly-defined process for research approval
- Patient-centred audit (but some staff concerns)
- Hospital staff can see recent GP test results
- Insistence on open data standards
- LOINC allows cumulative display for lab reports
- Access to history: user can view all previous versions of a report
- Radiology / Laboratory ordering (in production and in pilot)

What Worked Badly

- The repository is the sole record for hospital laboratory & radiology reports
- Doctors thought “copyto” was a safe communication channel
- Clinical staff cannot believe that they do not have a right to view their own records
- GPs were an afterthought

What We Have Learned

- Expect data errors
- Don't merge records – merge identities
- Need to plan for resilience
- Initial principle that “every user can see every record” has been compromised
- Users don't know what they don't know and they hate change
- Contributors will (try to) subvert open standards
- Desktop access should preserve user/patient context
- Data governance must be defined in advance

Further Information

www.privacy.org.nz/health-information-privacy-code/

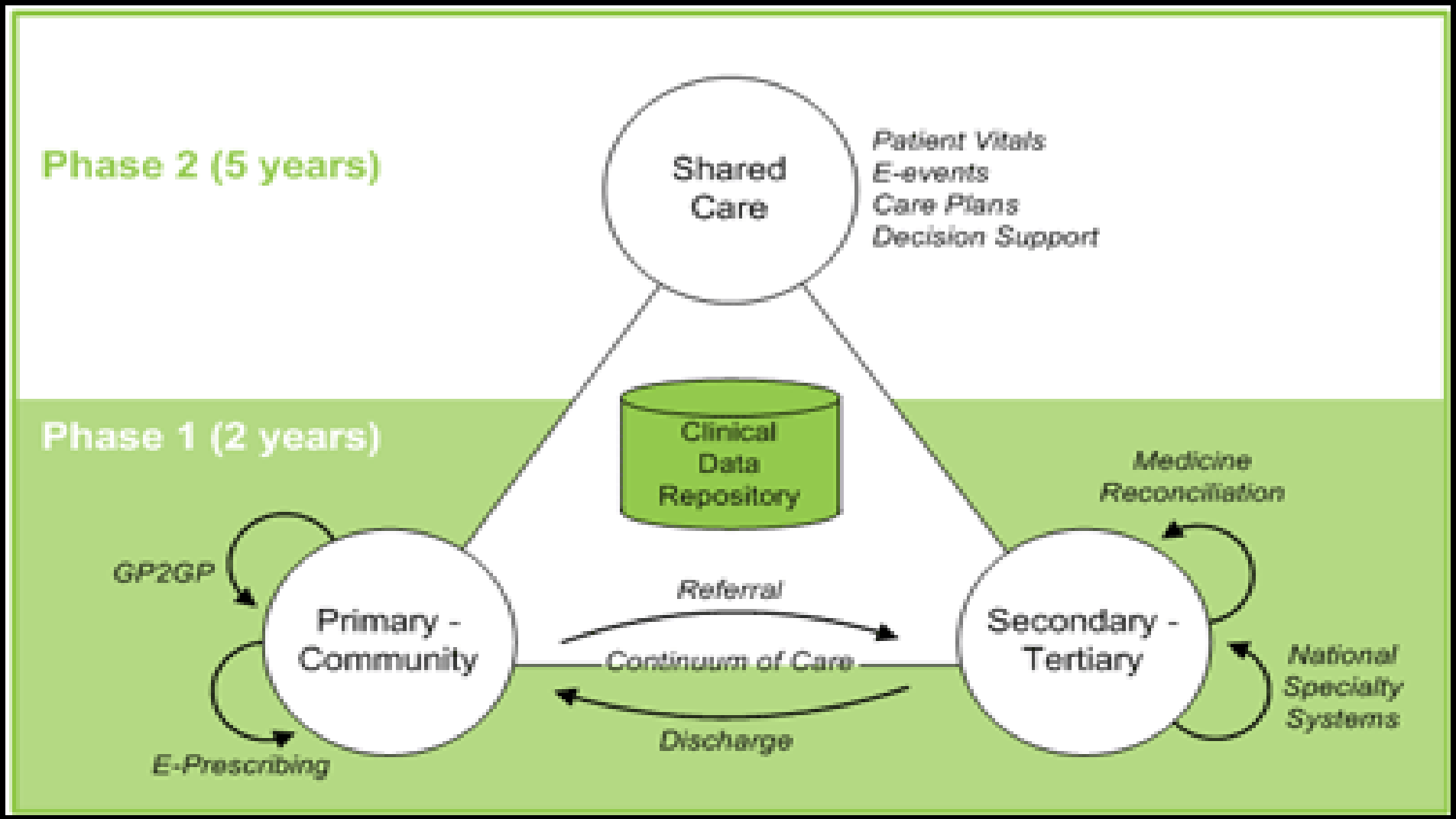
www.ithealthboard.health.nz

www.testsafe.co.nz

www.sysmex.co.nz/Eclair

Ross.Boswell@middlemore.co.nz

NZ National Health IT Board Vision



. . . and now for discussion

References:

www.testsafe.co.nz

www.sysmex.co.nz/eclair

www.nehta.gov.au/ehealth-implementation/pcehr-concept-of-operations

Contact:

Ross.Boswell@middlemore.co.nz

IT Issues for Practice Managers

Ross Boswell

Clinical Director of IT, CMDHB

Overview

Health Information Privacy Code

Information Security

NHITB Strategy and Regional Repositories

Health Information Privacy

Patient “owns” health information; practitioners and practices have stewardship of it

NZ Health Information Privacy Code requires practitioners to share information unless the patient forbids it

Health Information Security Framework

Section Heading	Description
Information Security Policy Refer section 5	This section explains that an organisation's management requires a policy for security management and that this policy should be reviewed on a regular basis.
Organising Information Security Refer section 6	This section describes what structures, agreements and responsibilities need to be in place to effectively implement information security practices within an organisation.
Asset Management Refer section 7	This section considers information as an asset requiring that health information be classified, handled, labelled and protected appropriately.
Human Resources Security Refer section 8	This section addresses the obligations of employees, contractors and third party users to protect and use information appropriately.
Physical and Environmental Security Refer section 9	This section addresses the physical access controls and appropriate housing for an organisation's information and information processing facilities.
Communications and Operations Management Refer section 10	This section addresses how information processing facilities should be operated in order to maintain adequate security.
Access Control Refer section 11	This section describes how access to information and information processing facilities should be controlled.
Information Systems Acquisition, Development and Maintenance Refer section 12	This section describes how security should be designed into systems, applications and operating procedures.
Information Security Incident Management Refer section 13	This section addresses how security incidents are to be reported, reviewed and learnt from.
Business Continuity Management Refer section 14	This section advises how to mitigate the effects of major systems failures and to make provision for recovery from such failures.
Compliance Refer section 15	This section discusses the obligations required to comply with the standard and legal requirements.

Information Security Policy

Responsibility	Procedure Description	Headline
Management	(a) Create and maintain the Information Security Policy document. It will be reviewed a minimum of every three years. *Recommended:* Visible support and commitment to security from all levels of management. *Recommended:* Make available to patients a summary of the security policy.	***Create and maintain an Information Security Policy***
Administrator	(a) Ensure that all new employees are aware of the Information Security Policy and kept informed of any changes and updates. *Recommended:* Provide advice and proactively promote the security policy.	***Develop employee awareness***
User	(a) Read, review, understand and follow obligations under the Information Security Policy.	***Follow user obligations***
System	(no requirements in this section)	

Information Security Policy Framework

7-page Microsoft Word framework document

Example section:

1.2.1 Objectives

[Typical objectives are outlined below. Edit as appropriate]

The objectives of [organisation] Information Security Policy are to preserve:

Confidentiality - information must not be made available or disclosed to unauthorised individuals, entities, or processes.

Integrity – data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes.

Availability – information must be accessible and useable on demand by authorised entities.