# STRENGTHENING PRIVACY AND CONFIDENTIALITY PROTECTION FOR ELECTRONIC HEALTH RECORDS

Michael Czapski
SeeBeyond Pty. Ltd
Australia
mczapski@seebeyond.com

Robert Steele
University of Technology, Sydney
Australia
rsteele@it.uts.edu.au

**ABSTRACT**
Inappropriate disclosure and use of personal health information could have severe adverse consequences for the individual to whom it pertains, but non-disclosure could adversely affect other individuals or the society. In Australia efforts are under way to develop legislation that will address the protection of confidential health information. Development of large-scale health information repositories, intended to facilitate access to health information to many more parties than was previously possible, makes the issue of consent enforcement and access control more urgent than ever. Literature suggests that the majority of security threats arise out of insider activities. It is proposed to develop a confidentiality protection framework that will ensure personal, identifiable health information is only disclosed by consent or under circumstances prescribed by law, and that all access to that information is audited. The framework, based on encryption of health information at the time of collection, and decryption at the time of authorised use, provides a number of advantages over the traditional, enterprise-centric protection model.

**KEY WORDS**
Electronic health records, security, privacy, encryption

## 1. Introduction

Although not without controversy [1, 2], privacy is considered an important civil right [3, 4] and personal information warrants protection through legislation [5].. As personal health information is considered the most sensitive kind of personal information [6], its protection is very important, particularly in the context of the emerging Electronic Health Records systems (EHRs).

EHRs have the potential for privacy and confidentiality breaches of a previously unseen severity. To gain the benefits of EHRs while minimising the risks requires *both* legislative and technological safeguards.

Current protection measures are inadequate. Existing systems employ standards and technologies that are based on the traditional, enterprise-centric security model that is not sufficient to address the issues posed by the EHRs. These issues are of immediate relevance to Australia-specific initiatives already under way, such as the Health*Connect* [7] and the Health e-link [8] initiatives, both of which have been criticized for relying on legislation without providing adequate technical measures [9-12].

This paper outlines the issues arising out of the implementation of EHRs and perceived threats to confidentiality of health information. It further proposes a confidentiality protection framework that would mitigate those threats and discusses its strengths and weaknesses.

## 2. Ethical and Legal Context

The notion of protecting confidentiality of health information is reputed to go back to 460 B.C. with the Hippocratic Oath containing an explicit passage to that effect [13].

It is expected that personal health information, shared in confidence with health workers, will remain confidential [14, 15].

Inappropriate disclosure of confidential health information can lead to long-term adverse psychological, social or financial consequences for the affected individuals. These range from embarrassment, through discrimination, threat of violence or death, to unwillingness to undergo medical treatment for fear of disclosure [16].

Disclosure of personal health information about one individual may affect other individuals. For example advances in genetic typing and research into hereditary diseases, coupled with inappropriate use of genetic information, may affect not just the individual to whom the information pertains but also their relatives. At the same time, lack of critical information, for example about allergies or communicable diseases, at critical times, may

lead to adverse consequences for the individual or the society.

Much legislative work was undertaken in recent years, both in Australia [6, 17-21] and abroad [21, 22], to establish legal frameworks for protection of personal health information. Both voluntary regulation [12] and the legislation currently in force in Australia are fragmented, differ from state to state and are considered inadequate [21, 23]. The draft National Health Privacy Code [17] is not yet a law. Its proposed provisions are already controversial [19] with some interest groups, most notably the Australian Medical Association [24], considering it too restrictive in some areas whilst not restrictive enough in others.

## 3. Related Work

There is evidence of a number of efforts to standardise electronic health records [25-27], ensure secure transmission of health records [28, 29], implement electronic health record repositories [21] and implement linkages between records from different sources [12].

The essential relationship between the electronic health information, privacy and legal protection frameworks is exemplified by the United States' Health Portability Accountability Act (HIPAA) and its explicit health information privacy protection provisions [22, 30].

In Australia, under the umbrella of the federal government's Health*Connect* initiative, a number of electronic health records trials are underway in Queensland, Tasmania and New South Wales[8, 16, 31]. Electronic Health Records systems are considered by their proponents as essential to improving healthcare [21, 31, 32],

## 4. Privacy and Confidentiality Threats

Whilst storage and access to records held by the Australian EHRs are subject to consent, and research into implementing consent systems has been undertaken in conjunction with these initiatives [14], issues such as, for example, transfer of ownership of records between parties are raising concerns [33].

Privacy risks posed by the proposed national EHRs are seen as severe [10] and the purported benefits, it is suggested, are lesser to patients than to other parties [16, 23, 34].

Literature suggests [35-37] that the majority of security threats arise out of insider activities. Numerous individuals, other than the information subjects and health workers, can access patient information, potentially bypassing audit and access control provisions of the systems that hold and purport to control access to those records.[9].

Significant advantages that can be derived by numerous parties, including governments and private sector organisations, from access to personal, identifiable health information, make those parties seek to gain access, not always by lawful means.

## 5. Issues

Personal health information about identifiable individuals is considerably different from other confidential information and must be treated differently.

Although owner-controlled information schemes were proposed and discussed [32, 38], most information about individuals is collected and stored in information systems not under the control of the information subject.

With some notable exceptions [39], confidentiality provisions of information systems [37, 40-42], including the Health*Connect*[7] and the Health e-link[8], are based on the traditional, enterprise-centric model of ownership and control [9, 43] where a single enterprise is the collector, the owner and the custodian of a collection of information. This model largely pre-determines data quality, system security and access control thinking, design and implementation.

Some of the implied assumptions, for example that information is collected within the organisation directly from individuals for internal organisational use, are challenged by the new electronic health record systems, that both call for routine transfer of patient information between General Practitioners, Hospitals and other healthcare settings, and for implementation of large-scale repositories, storing personal health information collected elsewhere. Confidentiality protection challenges of those systems suggest that a totally new approach must be developed. Security measures must be an integral part of information systems and must address known and expected security threats and exposures [9, 11, 15, 37]
Personal health information is typically collected as part of an encounter between the patient and the healthcare professional, by consent, and in confidence. With large volumes of data now held electronically it is however reasonably easy to mass duplicate records without detection if security and audit mechanisms are bypassed.

In addition to people involved in collecting and recording information and those who use it in the course of interaction with the subject, a great many other individuals may have access to confidential information, with, or without, explicit authorisation.

Even though the custodian enterprise may implement standards-compliant security policies [43], ensure that information is transmitted over secure channels[7, 8, 44], and do all that current best practices dictate, there still are individuals, who have no relationship to the information subject, who have access to information about them.

Mass record storage systems, mandated by the Health*Connect* and similar initiatives, intended to facilitate access by many parties who have not previously had access, further weakens the protection, assumed to exist when individuals agree to disclose their personal health information in confidence.

Whilst a number of standards and standards-based technologies have been applied to various areas of the problem domain[40-42, 44], and research has been conducted into confidentiality infrastructure [14, 45], there is no evidence of an effort to develop a comprehensive confidentiality protection framework.

## 6. Proposed Confidentiality Framework

### 6.1 Requirements

The following requirements should be recognized:

- apart from the need for health workers to access information about an identifiable individual during the course of interaction with those individuals, there is no need for that information to be viewable in a human-readable form.
- technology measures must back up the legislative provisions [14, 24].
- methods exist whereby information about identifiable individuals can be presented in a way such that it is still useable for research and statistical purposes but that it cannot be directly used to identify the individual
- aggregated and de-identified information can be made available for research and statistical purposes[15, 39, 45-47].

It is suggested that

- access to confidential health information should only be granted to those who have a patient-carer relationship with the subject and in relation to that relationship, or those who must have access under the law.
- under no circumstances should confidential health information be able to be viewed without consent or authorisation, and without secure audit trail.
- only a system that implements active measures to make it impossible to view protected information will satisfy the requirements and assist in enforcing health information privacy legislation.

### 6.2 Confidentiality Framework

It is proposed that a framework, based on encryption of stored records, combined with access audit mechanisms, would prevent accidental or deliberate disclosure and would facilitate prosecution of violators. To be practical, the framework must be built upon proven, effective technologies and must not impose excessive overheads.

Encrypting information at the point of capture and decrypting it at the point of use will satisfy the primary purpose of personal health information without exposing it to inappropriate disclosure.

The framework relies on a number of underlying concepts and infrastructure components described below.

*Health Information Classification Hierarchy* allows labelling of different parts of the record according to the sensitivity of the information they contain, clinical discipline, classes of health care workers that typically require access or the need to allow the subject to explicitly grant or deny access. Certain parts of the record would be labelled as 'mental health', 'sexual health', 'administrative' information or 'grant access to hospital care team'. Certain classifications would imply other classifications, for example mental health information would be a specialisation of general clinical information, allowing, for example, access granted to a specialised classification to also grant access to its superclass.

*Accessor Classification Hierarchy* places each potential accessor into one or more groups that can be granted or denied access to specific parts of the record according to the information classification hierarchy labels.

*Consent Hierarchy* allows the information subject to allow or deny access to specific parts of the record according to information sensitivity, clinical discipline, event type, for example hospitalisation, or any combination of the Health Information Classification Hierarchy labels.

Each record would be represented as a XML Instance Document [49], structured according to the Health Information Classification Hierarchy.

Specific parts of the record would be encrypted using techniques of the XML Encryption Specification[48] such that parts of the most confidential nature would be encrypted individually, possibly with different keys according to the classification labels, less critical parts would be encrypted independently, possibly causing superencryption of some parts, and finally the entire record, with some parts not yet encrypted, would be encrypted in its entirety. This process would take place at the point of record creation and would result in creation of an encrypted record, creation of a record entry in the global record index and the creation of a default consent entry in the global consent store.

Each record would be identified by a globally unique ID to facilitate, in conjunction with the hierarchy labels, location of appropriate encryption keys.

Encryption keys, accessor enrolment details, subject consent grants and access requests audit trail would be held independently of the encrypted records, and would be administered by one or more organisations established for the purpose.

Access to information contained in encrypted records would involve location and retrieval of the records, request for access, verification of requestor identity, verification of access grant, creation of an audit trail, retrieval of decryption keys and finally decryption of the appropriate parts of the record for viewing.

The supporting technology infrastructure would, at minimum, include a global, possibly federated, record index, participant register, consent store, encryption key store and audit trail store, each of which could, if desired, be independent, possibly administered by a different organisation. This infrastructure would be deployed at the

national level, or at minimum, at the level of a state, a region or a province.

As it is encrypted, the health record could be stored anywhere, and replicated, and transferred, with no concern for confidentiality.

The use of current common cryptographic algorithms, standards and technologies would satisfy the conditions of proven technology and minimal impact.

### 6.3 Advantages

The framework would address all the major issues associated with the electronic health record systems. Encryption will eliminate the possibility of casual disclosure and undetected data alteration. All access would be audited, and consent strictly enforced. Large volume data storage management, including replication, distribution and facility management outsourcing, could be implemented with a view to attaining the greatest efficiency and cost-effectiveness. Subsets of records could be distributed on compact disk, or similar media, to reduce demand for network bandwidth and expedite access.

### 6.4 Disadvantages

Encryption of health records would introduce issues not previously encountered. Most notably, complexity of applications used to view patient information would be increased. The application would need to contain the necessary mechanism to decrypt the data and validate its integrity.

It would be impossible to update old records – new records would need to be created with additional or changed information.

Separate infrastructure for research would have to be established and data would have to be specially prepared for inclusion in research stores, perhaps using pseudonymity and anonymity techniques and methods described in [39, 45, 46] and elsewhere

## 7 Conclusions

The legal framework for protection of confidential health information must be backed up by technological solutions that would implement appropriate protection measures.

Implementation of electronic health records systems, facilitating access to personal, identifiable health information to many more parties than previously possible, makes the requirement for implementation of adequate confidentiality protection, consent, access control and audit mechanisms an urgent issue.

The confidentiality protection framework proposed in this paper will ensure that confidential health information can only be viewed by consent, with authorisation or in circumstances prescribed by law, and that a complete audit trail is maintained.

Encrypting patient records at the point where they enter the electronic patient records systems, transmitting and storing these records in an encrypted form, and performing decryption only at the time and at the point of authorised use, will eliminate the possibility of casual disclosure.

Separating large volume data storage from storage and management of authorisation, consent and encryption keys will facilitate storage design that optimises cost and efficiency.

Of themselves, none of the concepts that form the framework are entirely new. The systematic assembly of those concepts into a comprehensive health information confidentiality framework is, we believe, what makes an important contribution to the field.

There are numerous technology applications, concepts and standards, both existing and yet to be developed, implied in the framework. An enormous amount of research is, and that is yet to be, undertaken in many areas to make the health information confidentiality framework practical. We trust that the research will continue to turn this vision into reality.

## References


[1] A. Mackenzie, "Politics of privacy, technologies of the political and the paradoxes of individuality", http://www.lancs.ac.uk/staff/mackenza/papers/privacy.pdf, Accessed: October 2004

[2] R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, Accessed: October 2004

[3] G. J. Walters, "Privacy and security: an ethical analysis," *SIGCAS Comput. Soc.*, vol. 31, pp. 8--23, 2001.

[4] B. Phillips, "The Newest and Oldest Human Right", http://www.stthomasu.ca/~ahrc/phillips.html, Accessed:

[5] "Privacy and the Public Sector - Government", http://www.privacy.gov.au/government/index.html, Accessed:

[6] "AUSTRALIANS ENCOURAGED TO COMMENT ON NEW HEALTH PRIVACY SAFEGUARDS", http://www.health.gov.au/internet/wcms/Publishing.nsf/Content/health-mediarel-yr2002-kp-kp02134.htm, Accessed: October 2004

[7] "Health*Connect* System Architecture," HealthConnect Program Office, Australian Government Department of Health and Ageing 2003.

[8] "EHR*Net Refined Requirements and Architecture Report", www.health.nsw.gov.au/im/ibs/ehr/documents/refined_requirements_architecturev2.1report.doc, Accessed: September 2002

[9] M. Czapski, "A question of confidence, not a question of trust. Better data confidentiality protection is necessary," presented at HIC 2004, Brisbane, Australia, 2004.

[10] Anonymous, "AMA Warning on Single National Health Database", http://www.ama.com.au/web.nsf/doc/WEEN-5GB45N, Accessed: October 2004

[11] "HealthConnect Interim Research Report and Draft Systems Architecture - Federal Privacy Commissioner Submission", http://www.privacy.gov.au/publications/healthcsub04.pdf, Accessed: January 2004

[12] Anonymous, "PANACEA OR PLACEBO ? - Linked Electronic Health Records and Improvements in Health Outcomes," NSW Ministerial Advisory Committee on Privacy and Health Information 2000.

[13] "Hippocratic Oath -- Classical Version", http://www.pbs.org/wgbh/nova/doctors/oath_classical.html, Accessed: October 2004

[14] "Electronic Consent Research - Summary of Final Reports", http://www7.health.gov.au/hsdd/primcare/it/docs/ecofinal.doc, Accessed: October 2004

[15] P. Armstrong, "Electronic Health Records: Privacy as an essential building block," in *Electronic Health Records: Privacy as an essential building block*. Sydney: Speach at the AFR 5th Health Congress, 2003.

[16] R. Clarke, "Research Challenges in Emergent e-Health Technologies", http://www.anu.edu.au/people/Roger.Clarke/EC/eHlthRes.html, Accessed: October 2004

[17] "Proposed National Health Privacy Code", http://www.health.gov.au/pubs/pdf/code.pdf, Accessed: August 2004

[18] "Guidelines on Privacy in the Private Health Sector", http://www.privacy.gov.au/publications/hg_01.html, Accessed: August 2004

[19] "Report on public submissions in relation to draft National Health Privacy Code", http://www.health.gov.au/pubs/pdf/report.pdf, Accessed: August 2004

[20] "Health Guidelines", http://www.privacy.gov.au/health/guidelines/index.html, Accessed: August 2004

[21] A. Cornwall, "ELECTRONIC HEALTH RECORDS: AN INTERNATIONAL PERSPECTIVE," *Health Issues Journal. Health Issues Centre Inc., La Trobe University*, 2002.

[22] Anonymous, "Summary of the HIPAA Privacy Rule", http://www.hhs.gov/ocr/privacysummary.pdf, Accessed:

[35] P. A. Miller, "Privacy in Cyberspace, with Prof. Arthur Miller - Medical Records", http://cyber.law.harvard.edu/privacy99/lesson8.html, Accessed: October 2004

[23] L. Beazley, "The Draft National Health Privacy Code", http://www.aar.com.au/pubs/bio/fohfeb03.htm, Accessed: October 2004

[24] "AMA submission on draft National Health Privacy Code", http://www.ama.com.au/web.nsf/doc/WEEN-5M462W, Accessed: October 2004

[25] O. J. Bott, ""The" Electronic Health Record - Standardization and Implementation", http://www.gpcg.org/databases/projectprint.asp?ID=252, Accessed: October 2004

[26] G. Paterson, M. Shepherd, X. Wang, C. Watters, and D. Zitner, "Using the XML-Based Clinical Document Architecture for Exchange of Structured Discharge Summaries," presented at Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 4, 2002.

[27] "Development of an XML Version of the HL7 Discharge and Referral Message (GPCG Project #23) Final Report", http://www.gpcg.org/publications/docs/projects2001/GPCG_Project23_01.PDF, Accessed:

[28] S. Auton, B. Blobel, K. Engel, P. Humenn, M. Kratz, M. Nolte, P. Pharow, G. Schadow, G. Seppala, V. Spiegel, M. Tucker, S. Wagner, and W. Wilson, "Health Level Seven Security Services Framework," HL7 Secure Transactions Special Interest Group - HL7 Organisation 1998.

[29] B. Blobel, V. Spiegel, P. Pharow, K. Ngel, and R. Krohn, "Standard Guide for Implementing EDI (HL7) Communication Security," Otto-von-Guericke University Magdeburg 1999.

[30] D. Baumer, J. B. Earp, and F. C. Payton, "Privacy of medical records: IT implications of HIPAA," *SIGCAS Comput. Soc.*, vol. 30, pp. 40--47, 2000.

[31] "A NSW Health Strategy for the Electronic Health Record - Government's Action Plan for Health", www.health.nsw.gov.au/im/ibs/chr/documents/chr_strategy_detailed.pdf, Accessed: August 2004

[32] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues", http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html, Accessed: October 2004

[33] K. Dearne, "Prescribing a privacy cure", http://www.consensus.com.au/ITWritersAwards/ITWarchive/ITWentries02/15KarenDearne.htm, Accessed: October 2004

[34] M. Carter, "Integrated electronic health records and patient privacy: possible benefits but real dangers", http://www.mja.com.au/public/issues/172_01_030100/carter/carter.html, Accessed: 178

[36] R. G. Smith, "Telemedicine and crime", http://www.aic.gov.au/publications/tandi/ti69.pdf, Accessed:

[37] T. Huston, "Security issues for implementation of e-medical records," *Commun. ACM*, vol. 44, pp. 89--94, 2001.

[38] C. Gates and J. Slonim, "Owner-controlled information," presented at Proceedings of the 2003 workshop on New security paradigms, 2003.

[39] A. Rector, "Clinical e-Science Framework: A New MRC-Funded Interdisciplinary Project," *Biomedical Informatics Today - NEWSLETTER OF THE BRITISH MEDICAL INFORMATICS SOCIETY*, 2002.

[40] M. Jurecic and H. Bunz, "Exchange of patient records-prototype implementation of a security attributes service in X.500," presented at Proceedings of the 2nd ACM Conference on Computer and communications security, 1994.

[41] B. Blobel, "Onconet: A Secure Infrastructure to Improve Cancer Patients' Care," *European Journal of Medical Research*, vol. 5, pp. 360-368, 2000.

[42] J. Halamka, P. Szolovits, and D. Rind, "A WWW Implementation of National Recommendations for Protecting Electronic Health Information," *J Am Med Inform Assoc*, vol. 4, pp. 458-464, 1997.

[43] "ISO/IEC 17799:2000 Information technology - Code of practice for information security management," in *ISO/IEC 17799:2000*, 2000.

[44] "Health Level Seven - Secure HL7 Transactions using Internet Mail," Health Level Seven Inc. 1999.

[45] Anonymous, "CLEF - integrating information for the clinical e-Scientist", http://www.clinical-escience.org/start.html, Accessed: October 2004

[46] R. Clarke, "Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue", http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html, Accessed:

[47] "Health informatics - Anonymity user requirements for trusted anonymisation facilities", http://www.centc251.org/TCMeet/doclist/TCdoc00/N00-013.pdf, Accessed:

[48] T. Imamura, B. Dillaway, and E. Simon, "XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002", W3C XML Encryption Working Group, World Wide Web Consortium, Available: http://www.w3.org/TR/xmlenc-core/, Accessed: April 2005.

[49] eXtensible Markup Language (XML), World Wide Web Consortium, Available: http://www.w3.org/XML/.

Proceedings of the IASTED International Conference
WEB TECHNOLOGIES, APPLICATIONS, AND SERVICES
July 4-6, 2005, Calgary, Alberta, Canada

# STRENGTHENING PRIVACY AND CONFIDENTIALITY PROTECTION FOR ELECTRONIC HEALTH RECORDS

Michael Czapski
SeeBeyond Pty. Ltd
Australia
mczapski@seebeyond.com

Robert Steele
University of Technology, Sydney
Australia
rsteele@it.uts.edu.au

**ABSTRACT**
Inappropriate disclosure and use of personal health information could have severe adverse consequences for the individual to whom it pertains, but non-disclosure could adversely affect other individuals or the society. In Australia efforts are under way to develop legislation that will address the protection of confidential health information. Development of large-scale health information repositories, intended to facilitate access to health information to many more parties than was previously possible, makes the issue of consent enforcement and access control more urgent than ever. Literature suggests that the majority of security threats arise out of insider activities. It is proposed to develop a confidentiality protection framework that will ensure personal, identifiable health information is only disclosed by consent or under circumstances prescribed by law, and that all access to that information is audited. The framework, based on encryption of health information at the time of collection, and decryption at the time of authorised use, provides a number of advantages over the traditional, enterprise-centric protection model.

**KEY WORDS**
Electronic health records, security, privacy, encryption

## 1. Introduction

Although not without controversy [1, 2], privacy is considered an important civil right [3, 4] and personal information warrants protection through legislation [5].. As personal health information is considered the most sensitive kind of personal information [6], its protection is very important, particularly in the context of the emerging Electronic Health Records systems (EHRs).

EHRs have the potential for privacy and confidentiality breaches of a previously unseen severity. To gain the benefits of EHRs while minimising the risks requires *both* legislative and technological safeguards.

Current protection measures are inadequate. Existing systems employ standards and technologies that are based on the traditional, enterprise-centric security model that is not sufficient to address the issues posed by the EHRs. These issues are of immediate relevance to Australia-specific initiatives already under way, such as the Health*Connect* [7] and the Health e-link [8] initiatives, both of which have been criticized for relying on legislation without providing adequate technical measures [9-12].

This paper outlines the issues arising out of the implementation of EHRs and perceived threats to confidentiality of health information. It further proposes a confidentiality protection framework that would mitigate those threats and discusses its strengths and weaknesses.

## 2. Ethical and Legal Context

The notion of protecting confidentiality of health information is reputed to go back to 460 B.C. with the Hippocratic Oath containing an explicit passage to that effect [13].

It is expected that personal health information, shared in confidence with health workers, will remain confidential [14, 15].

Inappropriate disclosure of confidential health information can lead to long-term adverse psychological, social or financial consequences for the affected individuals. These range from embarrassment, through discrimination, threat of violence or death, to unwillingness to undergo medical treatment for fear of disclosure [16].

Disclosure of personal health information about one individual may affect other individuals. For example advances in genetic typing and research into hereditary diseases, coupled with inappropriate use of genetic information, may affect not just the individual to whom the information pertains but also their relatives. At the same time, lack of critical information, for example about allergies or communicable diseases, at critical times, may

lead to adverse consequences for the individual or the society.

Much legislative work was undertaken in recent years, both in Australia [6, 17-21] and abroad [21, 22], to establish legal frameworks for protection of personal health information. Both voluntary regulation [12] and the legislation currently in force in Australia are fragmented, differ from state to state and are considered inadequate [21, 23]. The draft National Health Privacy Code [17] is not yet a law. Its proposed provisions are already controversial [19] with some interest groups, most notably the Australian Medical Association [24], considering it too restrictive in some areas whilst not restrictive enough in others.

## 3. Related Work

There is evidence of a number of efforts to standardise electronic health records [25-27], ensure secure transmission of health records [28, 29], implement electronic health record repositories [21] and implement linkages between records from different sources [12].

The essential relationship between the electronic health information, privacy and legal protection frameworks is exemplified by the United States' Health Portability Accountability Act (HIPAA) and its explicit health information privacy protection provisions [22, 30].

In Australia, under the umbrella of the federal government's Health*Connect* initiative, a number of electronic health records trials are underway in Queensland, Tasmania and New South Wales[8, 16, 31]. Electronic Health Records systems are considered by their proponents as essential to improving healthcare [21, 31, 32],

## 4. Privacy and Confidentiality Threats

Whilst storage and access to records held by the Australian EHRs are subject to consent, and research into implementing consent systems has been undertaken in conjunction with these initiatives [14], issues such as, for example, transfer of ownership of records between parties are raising concerns [33].

Privacy risks posed by the proposed national EHRs are seen as severe [10] and the purported benefits, it is suggested, are lesser to patients than to other parties [16, 23, 34].

Literature suggests [35-37] that the majority of security threats arise out of insider activities. Numerous individuals, other than the information subjects and health workers, can access patient information, potentially bypassing audit and access control provisions of the systems that hold and purport to control access to those records.[9].

Significant advantages that can be derived by numerous parties, including governments and private sector organisations, from access to personal, identifiable health information, make those parties seek to gain access, not always by lawful means.

## 5. Issues

Personal health information about identifiable individuals is considerably different from other confidential information and must be treated differently.

Although owner-controlled information schemes were proposed and discussed [32, 38], most information about individuals is collected and stored in information systems not under the control of the information subject.

With some notable exceptions [39], confidentiality provisions of information systems [37, 40-42], including the Health*Connect*[7] and the Health e-link[8], are based on the traditional, enterprise-centric model of ownership and control [9, 43] where a single enterprise is the collector, the owner and the custodian of a collection of information. This model largely pre-determines data quality, system security and access control thinking, design and implementation.

Some of the implied assumptions, for example that information is collected within the organisation directly from individuals for internal organisational use, are challenged by the new electronic health record systems, that both call for routine transfer of patient information between General Practitioners, Hospitals and other healthcare settings, and for implementation of large-scale repositories, storing personal health information collected elsewhere. Confidentiality protection challenges of those systems suggest that a totally new approach must be developed. Security measures must be an integral part of information systems and must address known and expected security threats and exposures [9, 11, 15, 37]

Personal health information is typically collected as part of an encounter between the patient and the healthcare professional, by consent, and in confidence. With large volumes of data now held electronically it is however reasonably easy to mass duplicate records without detection if security and audit mechanisms are bypassed.

In addition to people involved in collecting and recording information and those who use it in the course of interaction with the subject, a great many other individuals may have access to confidential information, with, or without, explicit authorisation.

Even though the custodian enterprise may implement standards-compliant security policies [43], ensure that information is transmitted over secure channels[7, 8, 44], and do all that current best practices dictate, there still are individuals, who have no relationship to the information subject, who have access to information about them.

Mass record storage systems, mandated by the Health*Connect* and similar initiatives, intended to facilitate access by many parties who have not previously had access, further weakens the protection, assumed to exist when individuals agree to disclose their personal health information in confidence.

Whilst a number of standards and standards-based technologies have been applied to various areas of the problem domain[40-42, 44], and research has been conducted into confidentiality infrastructure [14, 45], there is no evidence of an effort to develop a comprehensive confidentiality protection framework.

## 6. Proposed Confidentiality Framework

### 6.1 Requirements

The following requirements should be recognized:

- apart from the need for health workers to access information about an identifiable individual during the course of interaction with those individuals, there is no need for that information to be viewable in a human-readable form.
- technology measures must back up the legislative provisions [14, 24].
- methods exist whereby information about identifiable individuals can be presented in a way such that it is still useable for research and statistical purposes but that it cannot be directly used to identify the individual
- aggregated and de-identified information can be made available for research and statistical purposes[15, 39, 45-47].

It is suggested that

- access to confidential health information should only be granted to those who have a patient-carer relationship with the subject and in relation to that relationship, or those who must have access under the law.
- under no circumstances should confidential health information be able to be viewed without consent or authorisation, and without secure audit trail.
- only a system that implements active measures to make it impossible to view protected information will satisfy the requirements and assist in enforcing health information privacy legislation.

### 6.2 Confidentiality Framework

It is proposed that a framework, based on encryption of stored records, combined with access audit mechanisms, would prevent accidental or deliberate disclosure and would facilitate prosecution of violators. To be practical, the framework must be built upon proven, effective technologies and must not impose excessive overheads.

Encrypting information at the point of capture and decrypting it at the point of use will satisfy the primary purpose of personal health information without exposing it to inappropriate disclosure.

The framework relies on a number of underlying concepts and infrastructure components described below.

*Health Information Classification Hierarchy* allows labelling of different parts of the record according to the sensitivity of the information they contain, clinical discipline, classes of health care workers that typically require access or the need to allow the subject to explicitly grant or deny access. Certain parts of the record would be labelled as 'mental health', 'sexual health', 'administrative' information or 'grant access to hospital care team'. Certain classifications would imply other classifications, for example mental health information would be a specialisation of general clinical information, allowing, for example, access granted to a specialised classification to also grant access to its superclass.

*Accessor Classification Hierarchy* places each potential accessor into one or more groups that can be granted or denied access to specific parts of the record according to the information classification hierarchy labels.

*Consent Hierarchy* allows the information subject to allow or deny access to specific parts of the record according to information sensitivity, clinical discipline, event type, for example hospitalisation, or any combination of the Health Information Classification Hierarchy labels.

Each record would be represented as a XML Instance Document [49], structured according to the Health Information Classification Hierarchy.

Specific parts of the record would be encrypted using techniques of the XML Encryption Specification[48] such that parts of the most confidential nature would be encrypted individually, possibly with different keys according to the classification labels, less critical parts would be encrypted independently, possibly causing superencryption of some parts, and finally the entire record, with some parts not yet encrypted, would be encrypted in its entirety. This process would take place at the point of record creation and would result in creation of an encrypted record, creation of a record entry in the global record index and the creation of a default consent entry in the global consent store.

Each record would be identified by a globally unique ID to facilitate, in conjunction with the hierarchy labels, location of appropriate encryption keys.

Encryption keys, accessor enrolment details, subject consent grants and access requests audit trail would be held independently of the encrypted records, and would be administered by one or more organisations established for the purpose.

Access to information contained in encrypted records would involve location and retrieval of the records, request for access, verification of requestor identity, verification of access grant, creation of an audit trail, retrieval of decryption keys and finally decryption of the appropriate parts of the record for viewing.

The supporting technology infrastructure would, at minimum, include a global, possibly federated, record index, participant register, consent store, encryption key store and audit trail store, each of which could, if desired, be independent, possibly administered by a different organisation. This infrastructure would be deployed at the

national level, or at minimum, at the level of a state, a region or a province.

As it is encrypted, the health record could be stored anywhere, and replicated, and transferred, with no concern for confidentiality.

The use of current common cryptographic algorithms, standards and technologies would satisfy the conditions of proven technology and minimal impact.

### 6.3 Advantages

The framework would address all the major issues associated with the electronic health record systems. Encryption will eliminate the possibility of casual disclosure and undetected data alteration. All access would be audited, and consent strictly enforced. Large volume data storage management, including replication, distribution and facility management outsourcing, could be implemented with a view to attaining the greatest efficiency and cost-effectiveness. Subsets of records could be distributed on compact disk, or similar media, to reduce demand for network bandwidth and expedite access.

### 6.4 Disadvantages

Encryption of health records would introduce issues not previously encountered. Most notably, complexity of applications used to view patient information would be increased. The application would need to contain the necessary mechanism to decrypt the data and validate its integrity.

It would be impossible to update old records – new records would need to be created with additional or changed information.

Separate infrastructure for research would have to be established and data would have to be specially prepared for inclusion in research stores, perhaps using pseudonymity and anonymity techniques and methods described in [39, 45, 46] and elsewhere

## 7 Conclusions

The legal framework for protection of confidential health information must be backed up by technological solutions that would implement appropriate protection measures.

Implementation of electronic health records systems, facilitating access to personal, identifiable health information to many more parties than previously possible, makes the requirement for implementation of adequate confidentiality protection, consent, access control and audit mechanisms an urgent issue.

The confidentiality protection framework proposed in this paper will ensure that confidential health information can only be viewed by consent, with authorisation or in circumstances prescribed by law, and that a complete audit trail is maintained.

Encrypting patient records at the point where they enter the electronic patient records systems, transmitting and storing these records in an encrypted form, and performing decryption only at the time and at the point of authorised use, will eliminate the possibility of casual disclosure.

Separating large volume data storage from storage and management of authorisation, consent and encryption keys will facilitate storage design that optimises cost and efficiency.

Of themselves, none of the concepts that form the framework are entirely new. The systematic assembly of those concepts into a comprehensive health information confidentiality framework is, we believe, what makes an important contribution to the field.

There are numerous technology applications, concepts and standards, both existing and yet to be developed, implied in the framework. An enormous amount of research is, and that is yet to be, undertaken in many areas to make the health information confidentiality framework practical. We trust that the research will continue to turn this vision into reality.

## References


[1] A. Mackenzie, "Politics of privacy, technologies of the political and the paradoxes of individuality", http://www.lancs.ac.uk/staff/mackenza/papers/privacy.pdf, Accessed: October 2004

[2] R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, Accessed: October 2004

[3] G. J. Walters, "Privacy and security: an ethical analysis," *SIGCAS Comput. Soc.*, vol. 31, pp. 8--23, 2001.

[4] B. Phillips, "The Newest and Oldest Human Right", http://www.stthomasu.ca/~ahrc/phillips.html, Accessed:

[5] "Privacy and the Public Sector - Government", http://www.privacy.gov.au/government/index.html, Accessed:

[6] "AUSTRALIANS ENCOURAGED TO COMMENT ON NEW HEALTH PRIVACY SAFEGUARDS", http://www.health.gov.au/internet/wcms/Publishing.nsf/Content/health-mediarel-yr2002-kp-kp02134.htm, Accessed: October 2004

[7] "Health*Connect* System Architecture," HealthConnect Program Office, Australian Government Department of Health and Ageing 2003.

[8] "EHR*Net Refined Requirements and Architecture Report", www.health.nsw.gov.au/im/ibs/chr/documents/refined_requirements_architecturev2.1report.doc, Accessed: September 2002

[9] M. Czapski, "A question of confidence, not a question of trust. Better data confidentiality protection is necessary," presented at HIC 2004, Brisbane, Australia, 2004.

[10] Anonymous, "AMA Warning on Single National Health Database", http://www.ama.com.au/web.nsf/doc/WEEN-5GB45N, Accessed: October 2004

[11] "HealthConnect Interim Research Report and Draft Systems Architecture - Federal Privacy Commissioner Submission", http://www.privacy.gov.au/publications/healthcsub04.pdf, Accessed: January 2004

[12] Anonymous, "PANACEA OR PLACEBO ? - Linked Electronic Health Records and Improvements in Health Outcomes," NSW Ministerial Advisory Committee on Privacy and Health Information 2000.

[13] "Hippocratic Oath -- Classical Version", http://www.pbs.org/wgbh/nova/doctors/oath_classical.html, Accessed: October 2004

[14] "Electronic Consent Research - Summary of Final Reports", http://www7.health.gov.au/hsdd/primcare/it/docs/ecofinal.doc, Accessed: October 2004

[15] P. Armstrong, "Electronic Health Records: Privacy as an essential building block," in *Electronic Health Records: Privacy as an essential building block*. Sydney: Speach at the AFR 5th Health Congress, 2003.

[16] R. Clarke, "Research Challenges in Emergent e-Health Technologies", http://www.anu.edu.au/people/Roger.Clarke/EC/eHlthRes.html, Accessed: October 2004

[17] "Proposed National Health Privacy Code", http://www.health.gov.au/pubs/pdf/code.pdf, Accessed: August 2004

[18] "Guidelines on Privacy in the Private Health Sector", http://www.privacy.gov.au/publications/hg_01.html, Accessed: August 2004

[19] "Report on public submissions in relation to draft National Health Privacy Code", http://www.health.gov.au/pubs/pdf/report.pdf, Accessed: August 2004

[20] "Health Guidelines", http://www.privacy.gov.au/health/guidelines/index.html, Accessed: August 2004

[21] A. Cornwall, "ELECTRONIC HEALTH RECORDS: AN INTERNATIONAL PERSPECTIVE," *Health Issues Journal. Health Issues Centre Inc., La Trobe University*, 2002.

[22] Anonymous, "Summary of the HIPAA Privacy Rule", http://www.hhs.gov/ocr/privacysummary.pdf, Accessed:

[35] P. A. Miller, "Privacy in Cyberspace, with Prof. Arthur Miller - Medical Records", http://cyber.law.harvard.edu/privacy99/lesson8.html, Accessed: October 2004

[23] L. Beazley, "The Draft National Health Privacy Code", http://www.aar.com.au/pubs/bio/fohfeb03.htm, Accessed: October 2004

[24] "AMA submission on draft National Health Privacy Code", http://www.ama.com.au/web.nsf/doc/WEEN-5M462W, Accessed: October 2004

[25] O. J. Bott, ""The" Electronic Health Record - Standardization and Implementation", http://www.gpcg.org/databases/projectprint.asp?ID=252, Accessed: October 2004

[26] G. Paterson, M. Shepherd, X. Wang, C. Watters, and D. Zitner, "Using the XML-Based Clinical Document Architecture for Exchange of Structured Discharge Summaries," presented at Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 4, 2002.

[27] "Development of an XML Version of the HL7 Discharge and Referral Message (GPCG Project #23) Final Report", http://www.gpcg.org/publications/docs/projects2001/GPCG_Project23_01.PDF, Accessed:

[28] S. Auton, B. Blobel, K. Engel, P. Humenn, M. Kratz, M. Nolte, P. Pharow, G. Schadow, G. Seppala, V. Spiegel, M. Tucker, S. Wagner, and W. Wilson, "Health Level Seven Security Services Framework," HL7 Secure Transactions Special Interest Group - HL7 Organisation 1998.

[29] B. Blobel, V. Spiegel, P. Pharow, K. Ngel, and R. Krohn, "Standard Guide for Implementing EDI (HL7) Communication Security," Otto-von-Guericke University Magdeburg 1999.

[30] D. Baumer, J. B. Earp, and F. C. Payton, "Privacy of medical records: IT implications of HIPAA," *SIGCAS Comput. Soc.*, vol. 30, pp. 40--47, 2000.

[31] "A NSW Health Strategy for the Electronic Health Record - Government's Action Plan for Health", www.health.nsw.gov.au/im/ibs/ehr/documents/ehr_strategy_detailed.pdf, Accessed: August 2004

[32] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues", http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html , Accessed: October 2004

[33] K. Dearne, "Prescribing a privacy cure", http://www.consensus.com.au/ITWritersAwards/ITWarchive/ITWentries02/15KarenDearne.htm, Accessed: October 2004

[34] M. Carter, "Integrated electronic health records and patient privacy: possible benefits but real dangers", http://www.mja.com.au/public/issues/172_01_030100/carter/carter.html, Accessed: 178

[36] R. G. Smith, "Telemedicine and crime", http://www.aic.gov.au/publications/tandi/ti69.pdf, Accessed:

[37] T. Huston, "Security issues for implementation of e-medical records," *Commun. ACM*, vol. 44, pp. 89--94, 2001.

[38] C. Gates and J. Slonim, "Owner-controlled information," presented at Proceedings of the 2003 workshop on New security paradigms, 2003.

[39] A. Rector, "Clinical e-Science Framework: A New MRC-Funded Interdisciplinary Project," *Biomedical Informatics Today - NEWSLETTER OF THE BRITISH MEDICAL INFORMATICS SOCIETY*, 2002.

[40] M. Jurecic and H. Bunz, "Exchange of patient records-prototype implementation of a security attributes service in X.500," presented at Proceedings of the 2nd ACM Conference on Computer and communications security, 1994.

[41] B. Blobel, "Onconet: A Secure Infrastructure to Improve Cancer Patients' Care," *European Journal of Medical Research*, vol. 5, pp. 360-368, 2000.

[42] J. Halamka, P. Szolovits, and D. Rind, "A WWW Implementation of National Recommendations for Protecting Electronic Health Information," *J Am Med Inform Assoc*, vol. 4, pp. 458-464, 1997.

[43] "ISO/IEC 17799:2000 Information technology - Code of practice for information security management," in *ISO/IEC 17799:2000*, 2000.

[44] "Health Level Seven - Secure HL7 Transactions using Internet Mail," Health Level Seven Inc. 1999.

[45] Anonymous, "CLEF - integrating information for the clinical e-Scientist", http://www.clinical-escience.org/start.html, Accessed: October 2004

[46] R. Clarke, "Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue", http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html, Accessed:

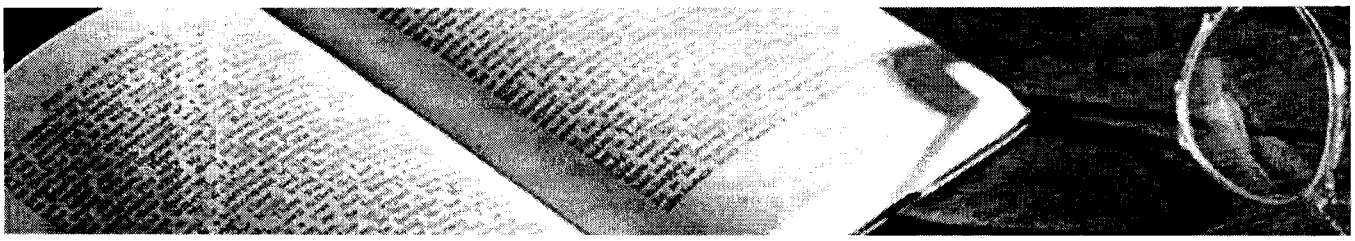
[47] "Health informatics - Anonymity user requirements for trusted anonymisation facilities", http://www.centc251.org/TCMeet/doclist/TCdoc00/N00-013.pdf, Accessed:

[48] T. Imamura, B. Dillaway, and E. Simon, "XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002", W3C XML Encryption Working Group, World Wide Web Consortium, Available: http://www.w3.org/TR/xmlenc-core/, Accessed: April 2005.

[49] eXtensible Markup Language (XML), World Wide Web Consortium, Available: http://www.w3.org/XML/.

ACTA Press

A Scientific and Technical Publishing Co






- Journals
- Proceedings
- Papers
- Subscriptions
- Submissions
- Call for Papers

Publication Search: Go

advanced search


# Web Technologies, Applications, and Services
## ~WTAS 2005~

**7/4/2005 - 7/6/2005**
**Calgary, Alberta, Canada**

**Editor(s):** M.H. Hamza
210 pages

**Rates (USD):**
$110.00 (Hardcopy);
$100.00 (Online);
$110.00 (CD)

**Individual Articles (USD):**
$20.00 (Online)

**ISSN:** N/A;
**ISBN:** 0-88986-483-7;
**ISSN (CD):** N/A;
**ISBN (CD):** 0-88986-485-3

IASTED

The IASTED Conference on **Web Technologies, Applications, and Services**
**Calgary, Alberta, Canada**
**July 17-19, 2006**

**Please choose a year:** 2005

**Add to Shopping Cart**

Hardcopy | Online Subscription | CD

*Abstracts may contain minor errors and formatting inconsistencies. Please contact us if you have any concerns or questions.*

| Track - Web-Based Applications | Free | Subscr |
|---|---|---|
| **494-038 An Evolvable, Composable Framework for Rapid Application Development and Dynamic Integration of Medical Image Processing Web Services**<br>*T. Mitsa and P. Joshi (USA)* | Abstract | Buy no |
| **494-043 WebFace: A Web-based Facial Animation System**<br>*M. Al-Marri, A. Al-Qayedi, and R. Benlamri (UAE)* | Abstract | Buy no |
| **494-079 Load Balancing Grid Computing Middleware**<br>*A. Touzene, S. Al Yahyai, K. Day, and B. Arafeh (Sultanate of Oman)* | Abstract | Buy no |
| **494-081 Post-Deployment Specification, Analysis and Testing of Enterprise Web Applications**<br>*W. Haque, A. Kranz, and R.A. Lucas (Canada)* | Abstract | Buy no |