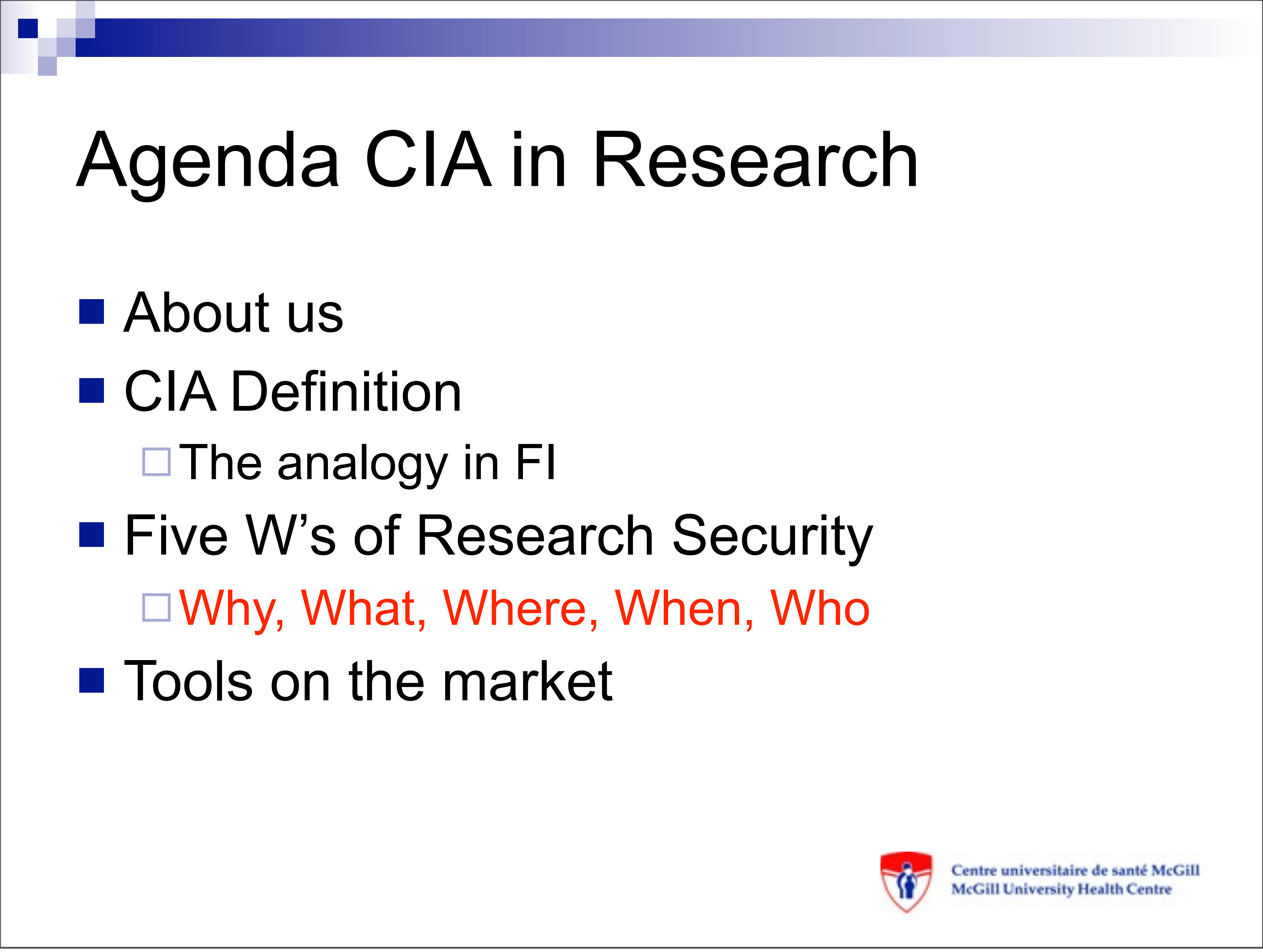
Privacy and Confidentiality in Health Research: What You Should Know

Subtitle: Confidentiality, Integrity & Availability
Author: Martin Fiset

Date: April 14 2011

Centre universitaire de santé McGill
McGill University Health Centre



Agenda CIA in Research

- About us
- CIA Definition
  - The analogy in FI
- Five W's of Research Security
  - Why, What, Where, When, Who
- Tools on the market

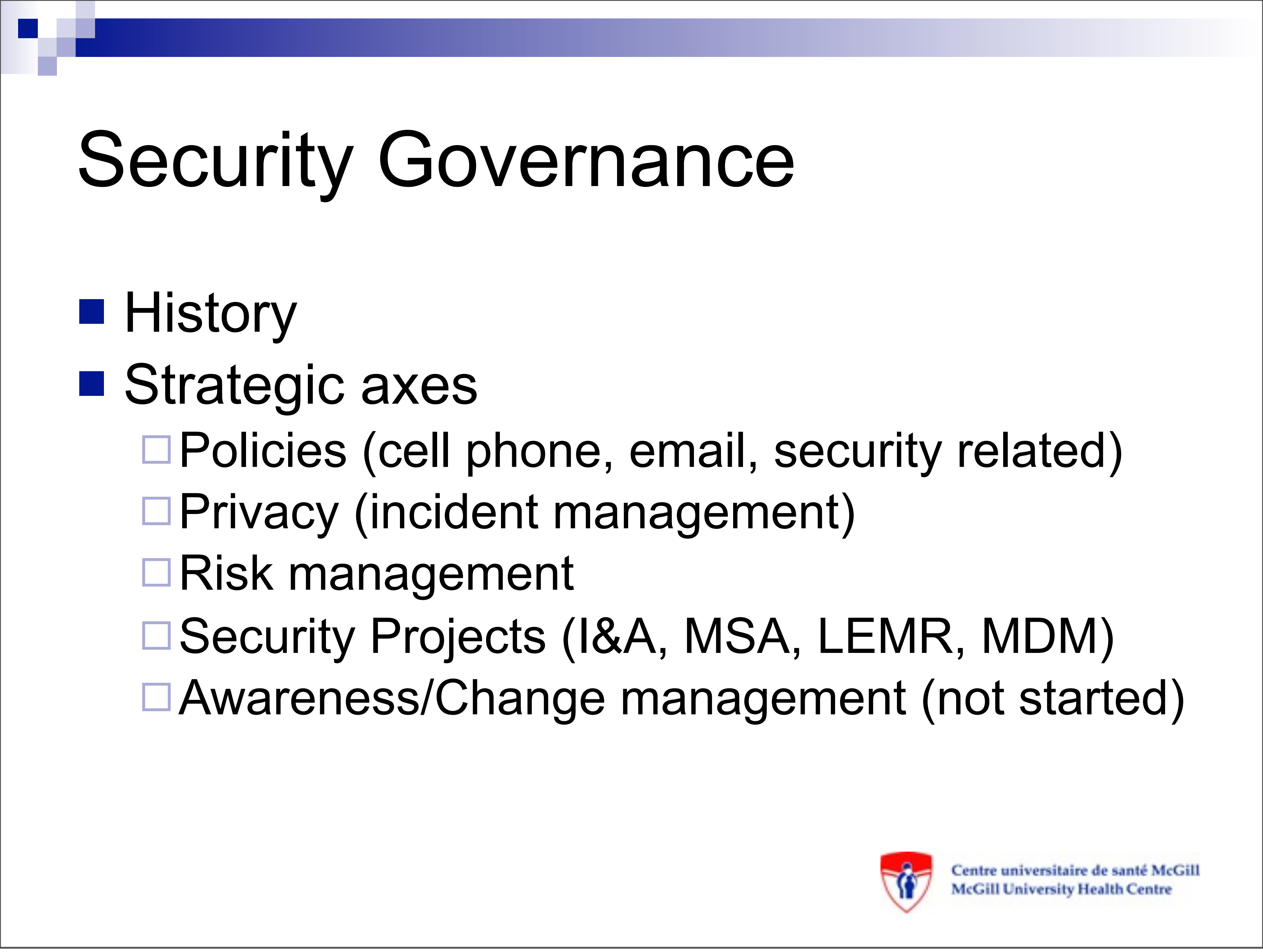
Centre universitaire de santé McGill
McGill University Health Centre

Bonjour,

First I'd like to thank Linda Furlini & Doctor Cournoyer for giving me a chance to talk with you today. Considering my background, it is kind of a miracle that we are sitting in the same room today.

I'm a clear advocate of "thinking outside the Box" & what we are about to talk today, will certainly have this effect on you.

It isn't my wish to turn you into security experts, but it is my intention of giving you enough concepts & tools so that you can have a pretty good understanding of the ins & out of IT security in the context of health research.



Security Governance

- History
- Strategic axes
  - □ Policies (cell phone, email, security related)
  - □ Privacy (incident management)
  - □ Risk management
  - □ Security Projects (I&A, MSA, LEMR, MDM)
  - □ Awareness/Change management (not started)

Centre universitaire de santé McGill
McGill University Health Centre

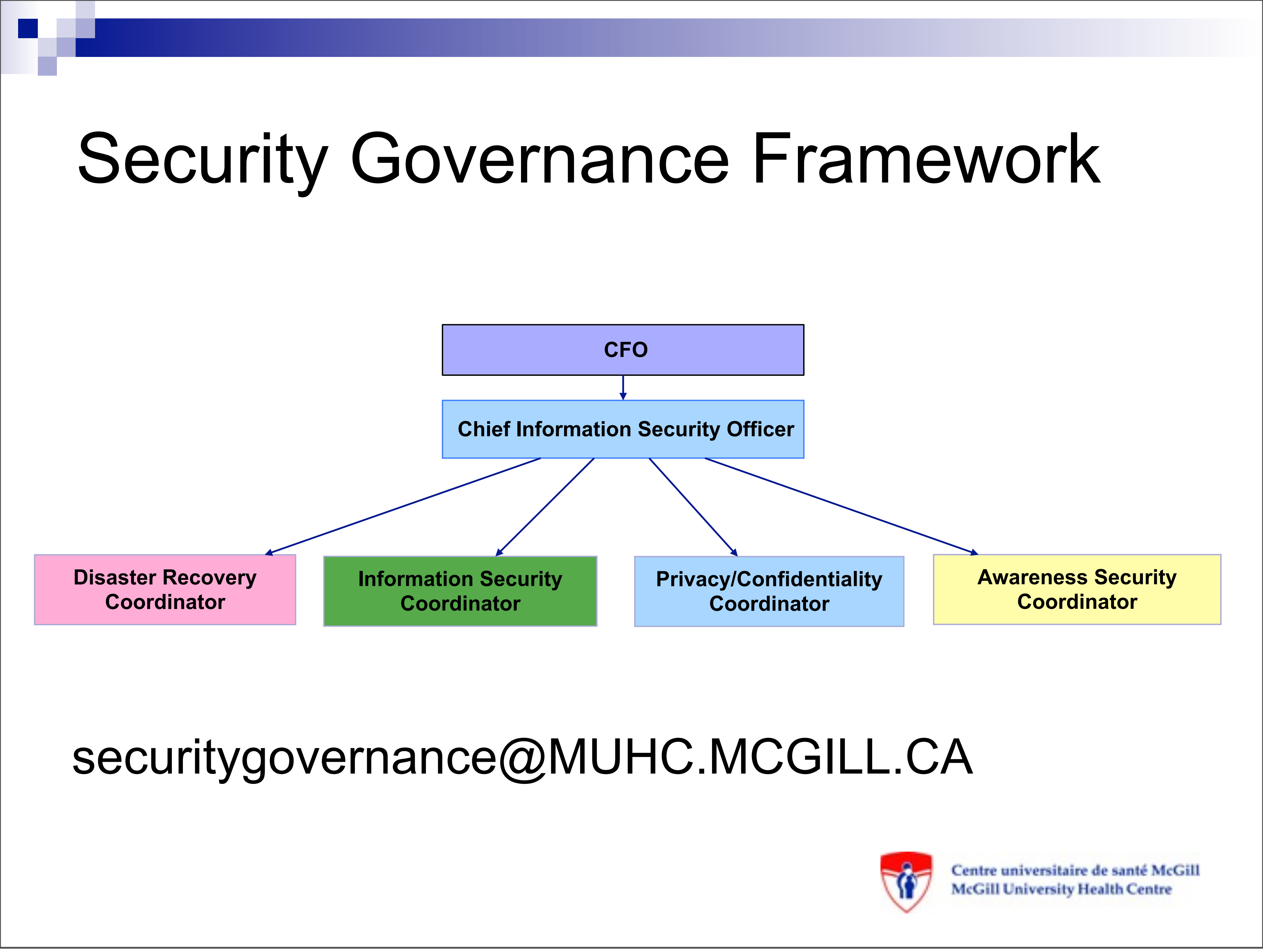
Bonjour,

As you know, my name is Martin Fiset & I'm a consultant working within MUHC's Security Governance Group. This group is concerned with Information Security & not only in relation with IT.

We owe our existence to a bug that brought down the Health network back in 2007. At that time, there wasn't any real security governance within the MSSS and even less within the RUIS. At MUHC, there was a few IT people with some interest in security but no real structure existed.

After that event, it was decided that security governance was a necessity within our grounds.

Since then, we are now working actively at trying to prepare MUHC's infrastructure to support the future, that is medical files that are all digital, hence one of our projects called eLMR (Legal Electronic Medical Record)



Security Governance Framework

CFO

Chief Information Security Officer

Disaster Recovery Coordinator

Information Security Coordinator

Privacy/Confidentiality Coordinator

Awareness Security Coordinator

securitygovernance@MUHC.MCGILL.CA

Centre universitaire de santé McGill
McGill University Health Centre

Our group (SG) is still small, 4 permanent employees (including our Manager Sylvie Beausoleil). We report directly to Rene Carignan our CFO.

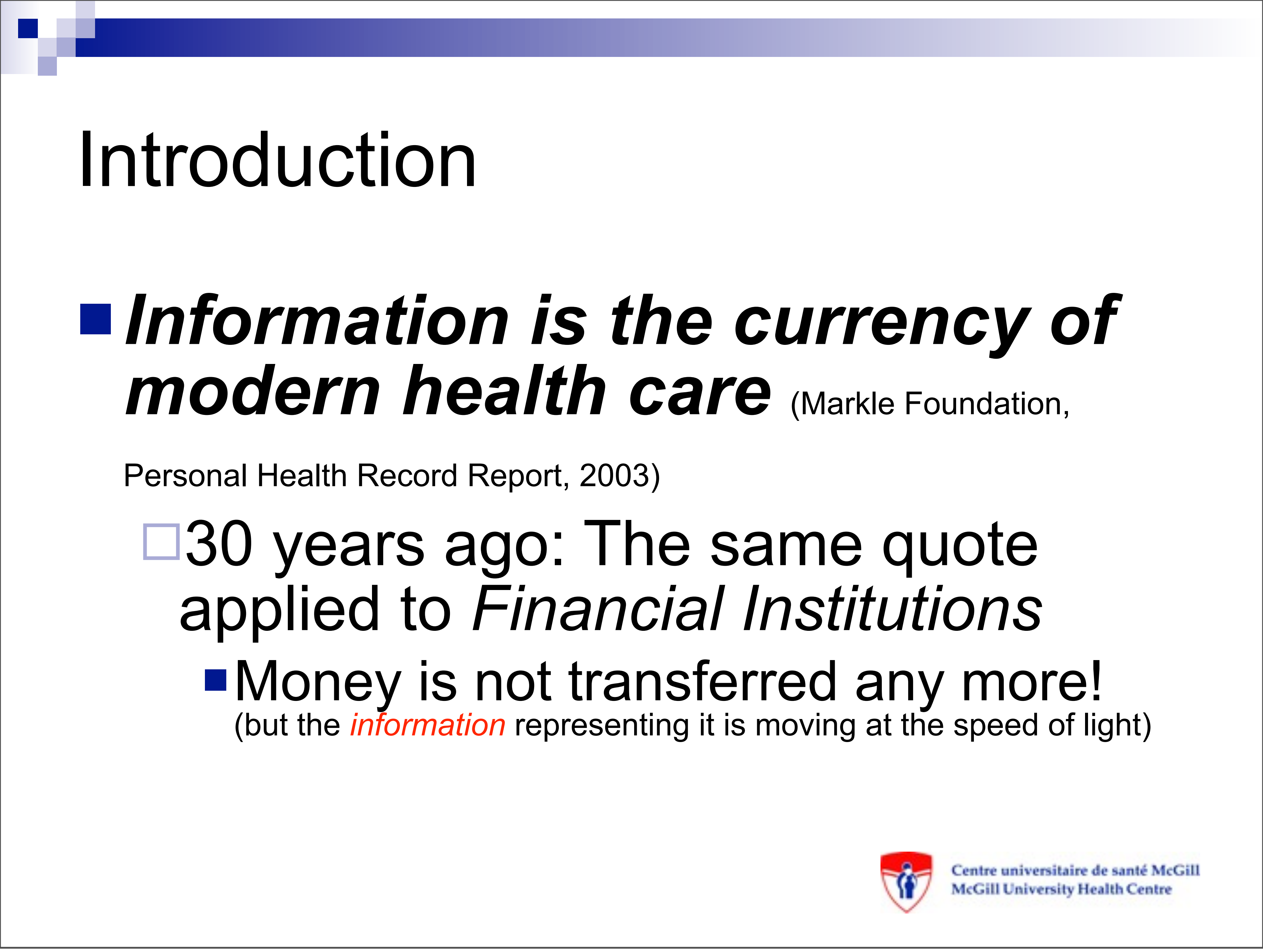
Most of us are consultants from outside. In fact, we only have one permanent employee, but he's quite a number. It seems security & health don't really mix together.

I can understand why; security can be viewed as a show stopper for IT projects.

My idea is that we have here an issue with perception.

It would be impossible for FIs (Financial Institutions) to have that many payment options (and ways to charge fees) if it wasn't for security. Security is an enabler of new businesses from my point of view.

SG's role within MUHC as always been that of a catalyst for change. And given the importance of security in the Health sector, confidentiality is paramount.



Introduction

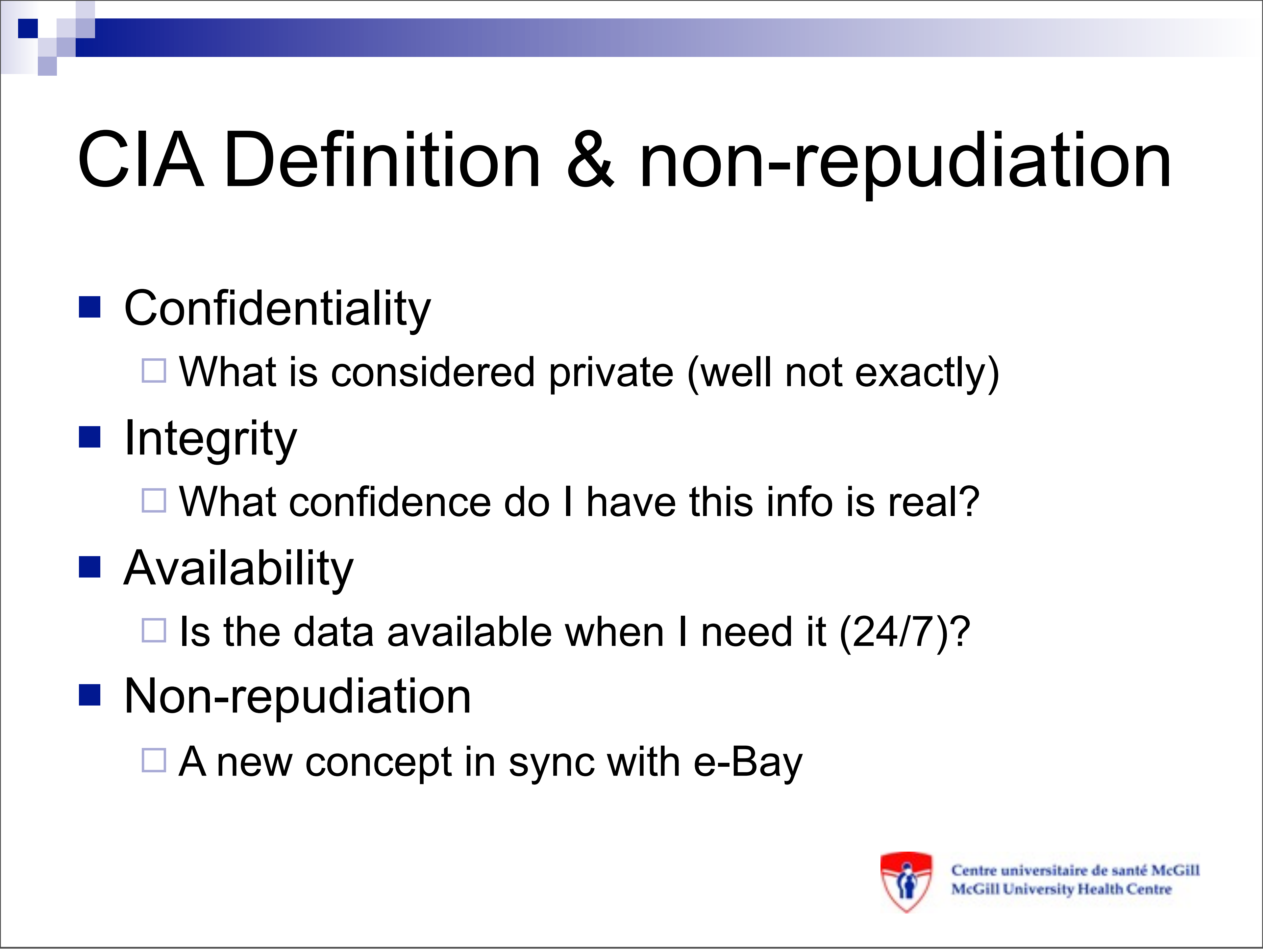
- ***Information is the currency of modern health care*** (Markle Foundation, Personal Health Record Report, 2003)
  - □30 years ago: The same quote applied to *Financial Institutions*
    - Money is not transferred any more! (but the *information* representing it is moving at the speed of light)

Centre universitaire de santé McGill
McGill University Health Centre

To further push this comparison I started with Financial Institutions. I have to make a confidence that this is the industry that oriented my career in IT security.

As I was searching for laws, regulations & general principles about Health Research, I came across this statement from the Markle Foundation in the USA. That’s strange I though to myself that we used to say this within the financial world. It is not paper money that is traveling any more, it is the information pertaining to money…

How did we get there & how did we manage to limit the impact of this transition from paper money to digital information about money?



CIA Definition & non-repudiation

- Confidentiality
  - □ What is considered private (well not exactly)
- Integrity
  - □ What confidence do I have this info is real?
- Availability
  - □ Is the data available when I need it (24/7)?
- Non-repudiation
  - □ A new concept in sync with e-Bay

Centre universitaire de santé McGill
McGill University Health Centre

How did we get there & how did we manage to limit the impact of this transition from paper money to digital information about money?

To answer the question we need to introduce some concepts. Like CIA. Everything we do in security (mostly for IT security) is based on these concepts of Confidentiality, Integrity & Availability. The last concept is relatively new & is a direct consequence of doing business on the internet.

We probably each have our own idea of a definition for these terms. Let me put it in simple terms for the purpose of this talk.

Confidentiality refers to the protection of the information. Normally your health record is to be viewed only by your physician & those that need to assist this person & ensuring your proper treatment within our walls. I’ve heard that here you are only allowed to see what your job definition allows you to see.

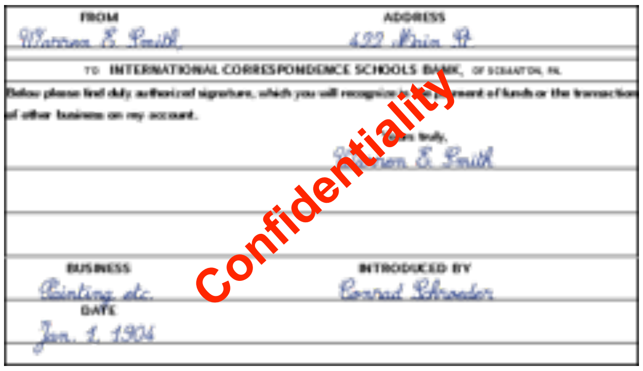
Integrity is a measure of our assurance that no data modification occurred that isn’t accounted for.

Availability is mostly a concern for the manager of IT operations, but it also rings a bell for security as it refers to being able to process transactions in which security plays a permanent role.
Finally non-repudiation refers to an event that occurred in the past for which we have an irrefutable trace that the event did occur. There is a pretty good application of this here within our walls when we start talking about Electronic Signatures & how it is implemented presently.

Yesterday's Bricks & Mortar

Bankbook

+



FROM: Warren E. Smith
ADDRESS: 422 Main St.

TO INTERNATIONAL CORRESPONDENCE SCHOOLS BANK, OF SCRANTON, PA.

Below please find duly authorized signature, which you will recognize in the payment of funds or the transaction of other business on my account.

Yours truly,
Warren E. Smith

BUSINESS: Painting, etc.
INTRODUCED BY: Conrad Schroeder
DATE: Jan. 1, 1904

Confidentiality

Signature card

=

Opening Hours
8am – 9pm
Monday – Saturday
9am – 6pm
Sundays & Public Holidays

Availability

Centre universitaire de santé McGill
McGill University Health Centre

Yesterday's Banking market was all paper based just like our Health system today.

Back then, the CIA triad applied to physical elements.

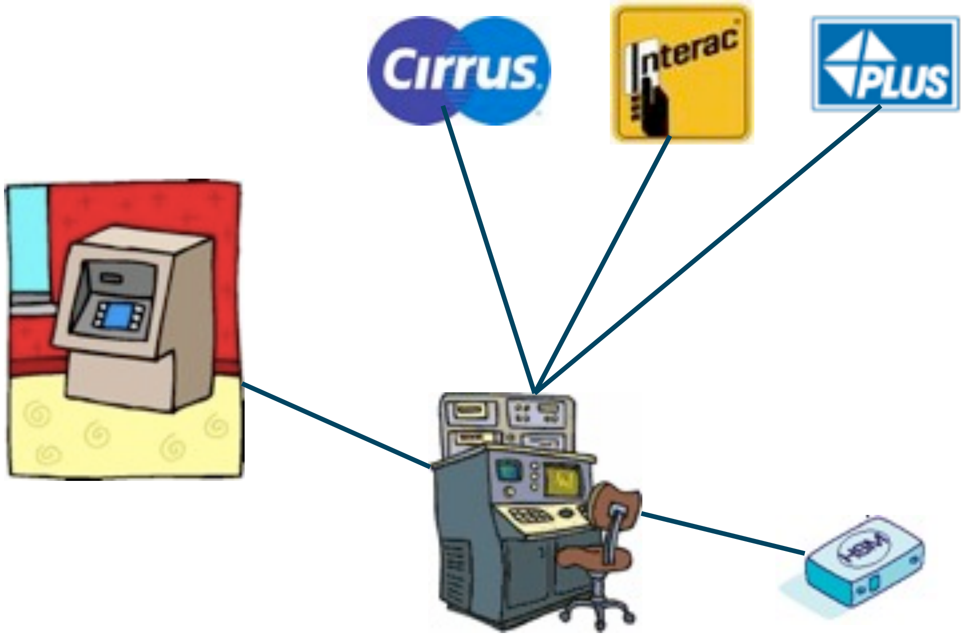
Confidentiality referred to your signature card. Integrity to the your bankbook & the mainframe that held the same information. Finally Availability was a question of the branches opening hours.

We could say that everything was paper based, just like patient charts. I still remember my first Caisse Populaire livret des transactions which was hand written by the bank clerk at the time. & I'm not that old!!!

Today’s Banking Industry

+ PIN

=



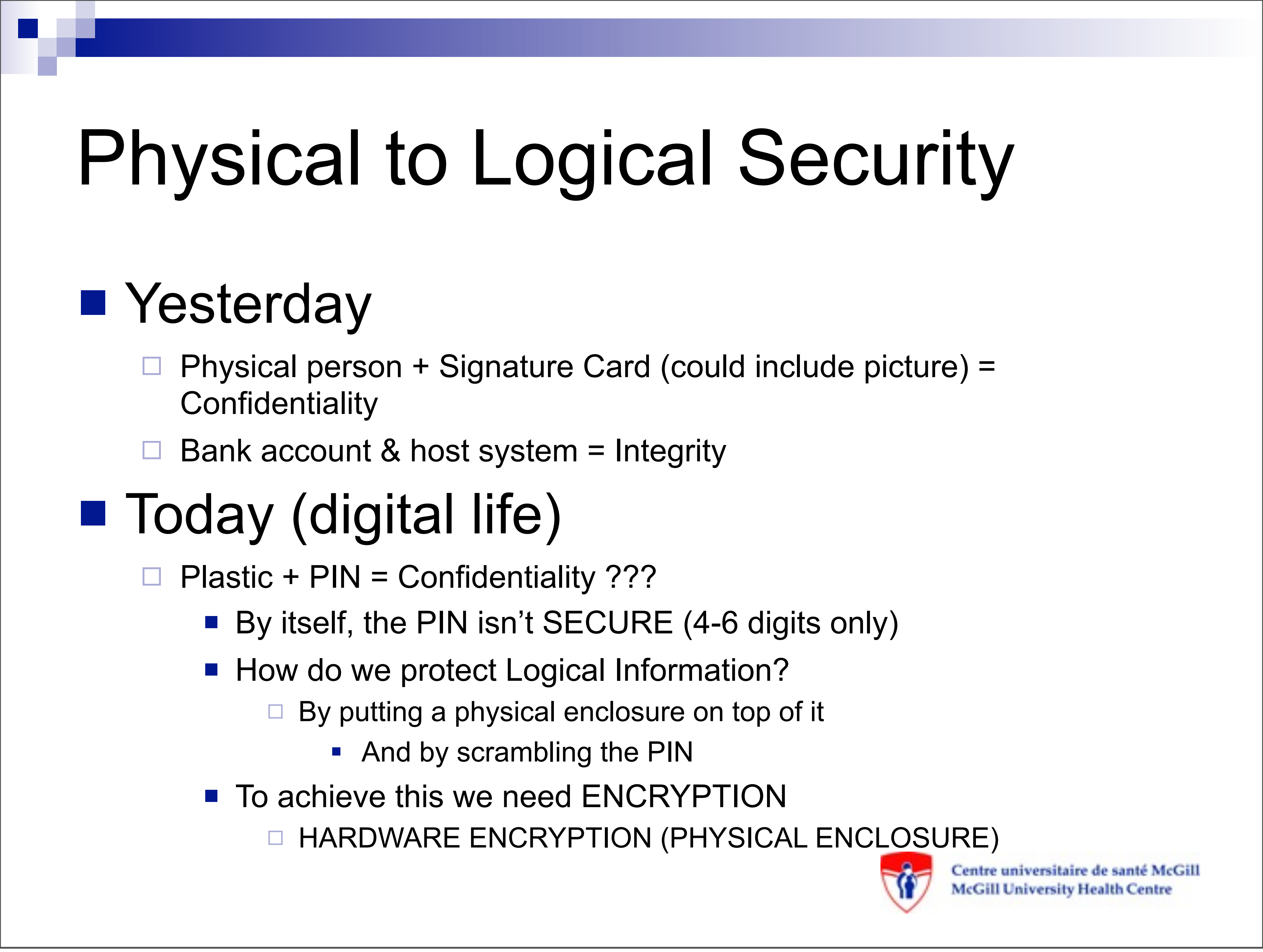
Centre universitaire de santé McGill
McGill University Health Centre

Today with just a plastic & a 4 digit PIN, you can get money from any bank machine from any place in the world!!! And you get instant access to whatever value you have with an FI which his located near your home.

Wouldn’t that be great if your Health Charts were available the same way? And of course only to those who need access to the information. Without a security architecture this is impossible.

So how is it that even though banks compete with each other, they still put trust in this relationship of sharing banking machines & payment systems all around the world???? Of course SECURITY is the reason.

And the way the system is built, you can trust your competition because they have to comply to the same security infrastructure that prevents fraud.



Physical to Logical Security

- Yesterday
  - Physical person + Signature Card (could include picture) = Confidentiality
  - Bank account & host system = Integrity
- Today (digital life)
  - Plastic + PIN = Confidentiality ???
    - By itself, the PIN isn’t SECURE (4-6 digits only)
    - How do we protect Logical Information?
      - By putting a physical enclosure on top of it
        - And by scrambling the PIN
    - To achieve this we need ENCRYPTION
      - HARDWARE ENCRYPTION (PHYSICAL ENCLOSURE)

Centre universitaire de santé McGill
McGill University Health Centre

Now let’s go back to what we want to achieve.

We want to move from a Paper based system to a logical based system. Physical to logical.

How did we manage this? With a SECURITY INFRASTRUCTURE.

There is a need to understand what replaced what.

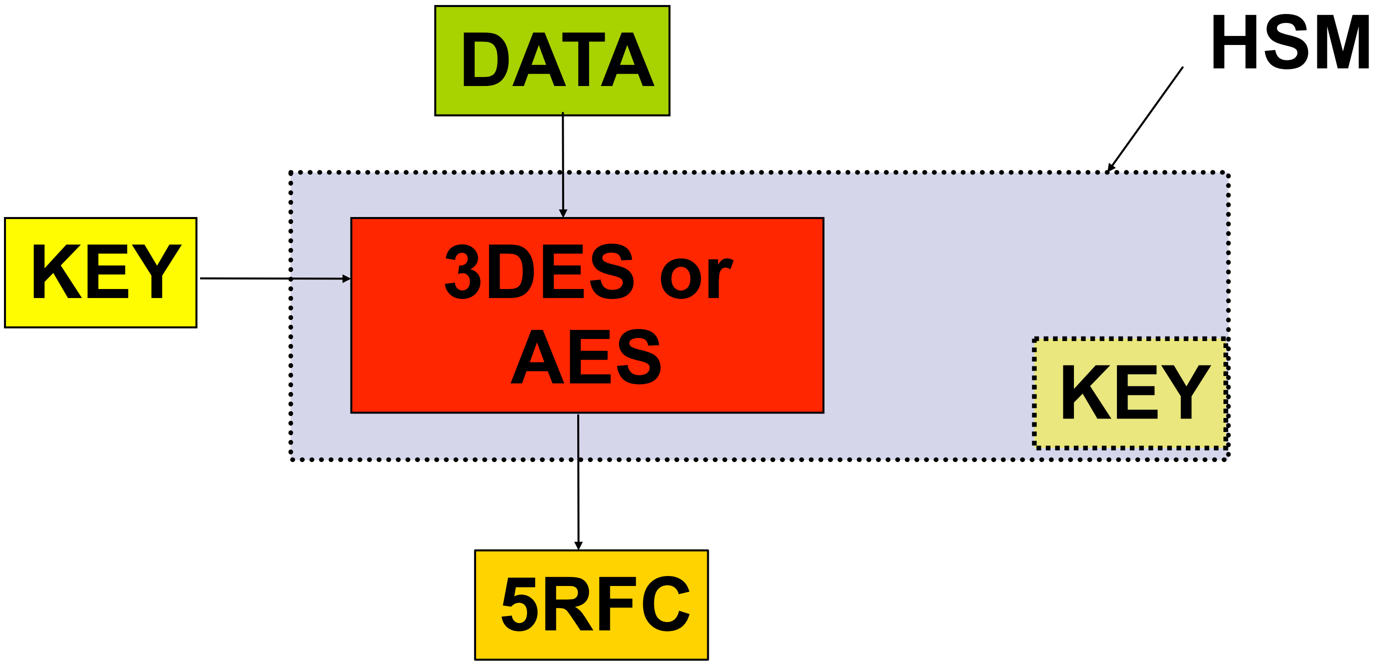
The passbook or bankbook is now a plastic. Your signature is now your PIN. And the bank hours are now your own (24/7), & we don’t expect anything less.

I used to sell these HSM (Hardware Security Module): We had the analogy of saying that a HSM is by definition a VAULT for which you have physical keys to protect it’s content, just like a real physical Vault.

A few years ago National Bank was a hub for the distribution of paper money to
Eastern Canada. Today their HUGE VAULT (600 DeLaGauchetiere) is used to store furniture & old PCs.

What is ENCRYPTION?

- Using a **known Algorithm** to scramble information



Centre universitaire de santé McGill
McGill University Health Centre

We have to distinguish various types of Encryption Algos.

Symmetrical & Asymmetrical:

The same key is used to encrypt & decrypt: 3DES & AES are Symmetrical

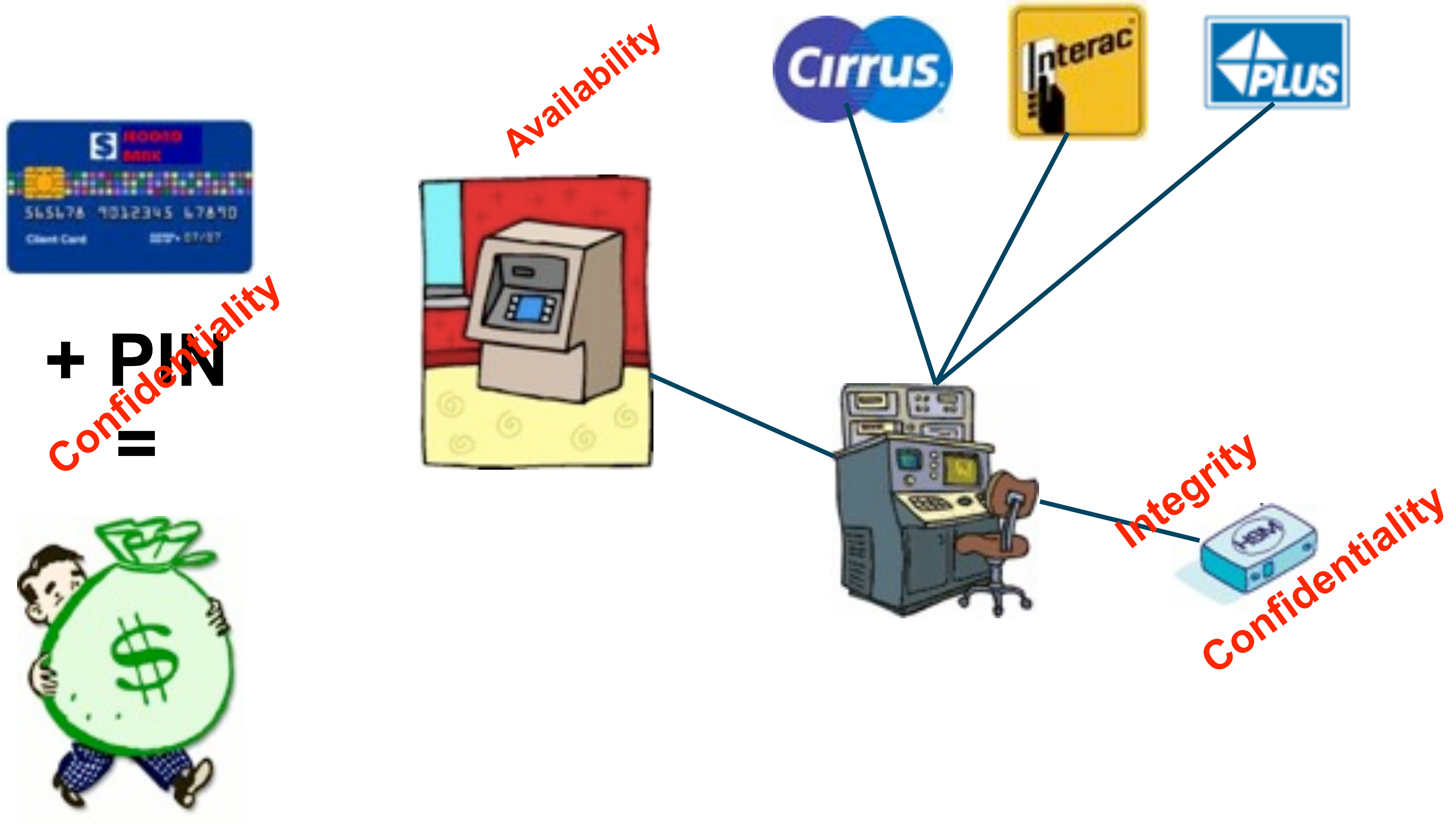
A different key is used for encrypt/decrypt: RSA & ECC are asymmetrical:

Asymmetrical algos are used for eSignatures, key distribution, cell phones, Symmetrical systems are used extensively in the banking & insurance world.

We also need to say that in cryptology we only trust an algorithm for which there was enough testing done by peers.

A cryptogram is when we talk about a piece of information that is encrypted. For example we can talk about a KEY CRYPTOGRAM. In theory there is only one key that needs injection inside the HSM; the Master File Key or MFK. All the other keys are encrypted under the MFK. By doing this, we can store the cryptogram of a KEY in any database location with no other protection; the key is encrypted!

Today’s Banking Industry



Centre universitaire de santé McGill
McGill University Health Centre

Let’s go back to our previous image. We can now say with certainty that the PIN is always protected as soon as it enters the FI network. There is no way of getting that clear value. Only a encrypted PIN travels the network. And the validation is done within the HSM. Period.

Integrity is also a ‘’by-product’’ of hardware encryption. We use a function called a MAC (Message authentication Code) to confirm the integrity of a transaction.

Non-repudiation is not a function of those systems. It normally includes some sort of secured timestamp.

Crypto Banking Principles

1. Pins never in clear
2. Keys never in clear (Hardware)
3. Key Mgnt Automated
4. Not possible to turn against itself

Centre universitaire de santé McGill
McGill University Health Centre

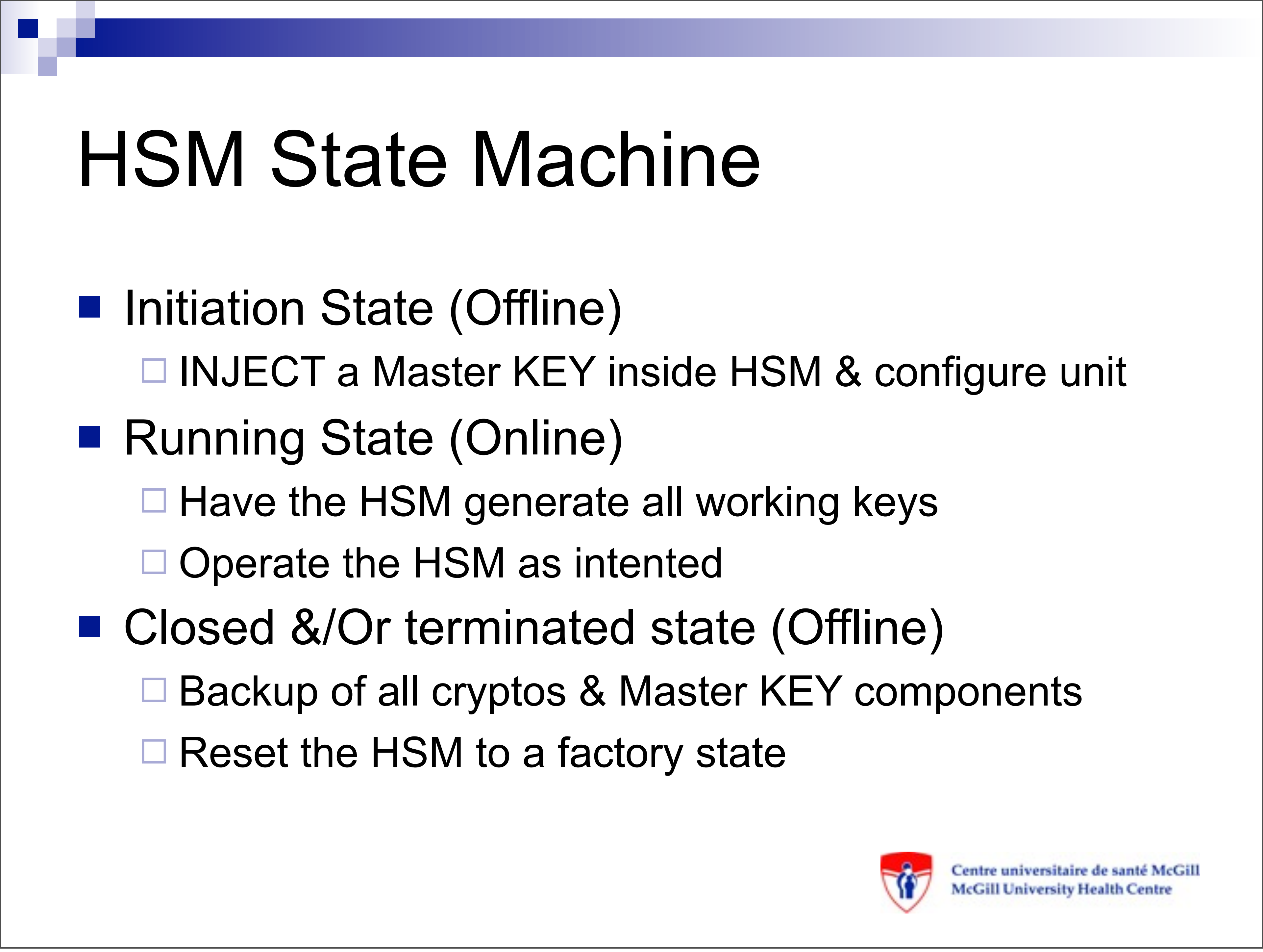
Commercial Hardware Security Modules or HSM appeared on the market only in the 70s. Initially just for the military, they were still regulated by the same restrictions as ballistic missiles up till the beginning of the 90s.

The first commercial HSMs were capable of dealing with PINs & Money. Their capacity of dealing with simple data encryption was pretty limited, if not totally impossible. Today’s functions are available to everyone on a simple USB KEY. Imagine, from a 35K$ HSM (back in 1987) to a 40$ USB secured key.

A few years ago, it was still not permitted to use encrypted messages in some countries (like France). The inventor of PGP (Pretty Good Privacy) was jailed in the US after releasing his code on the internet.

Going back to the slide:

We have to view the HSM as a VAULT. We store keys & algos in the box & we limit the interactions that are possible with the box (In/Out function). For instance, we can verify that a PIN is valid, but we can never extract a CLEAR PIN from the HSM.



HSM State Machine

- Initiation State (Offline)
  - □ INJECT a Master KEY inside HSM & configure unit
- Running State (Online)
  - □ Have the HSM generate all working keys
  - □ Operate the HSM as intented
- Closed &/Or terminated state (Offline)
  - □ Backup of all cryptos & Master KEY components
  - □ Reset the HSM to a factory state

Centre universitaire de santé McGill
McGill University Health Centre

An HSM is a state machine. In other words, when it is first delivered & installed, the unit is in a factory state mode. It will interact with the outside world once it is connected, however, it won't be able to process any cryptographic functions until the unit is initialized.

Initiation State:

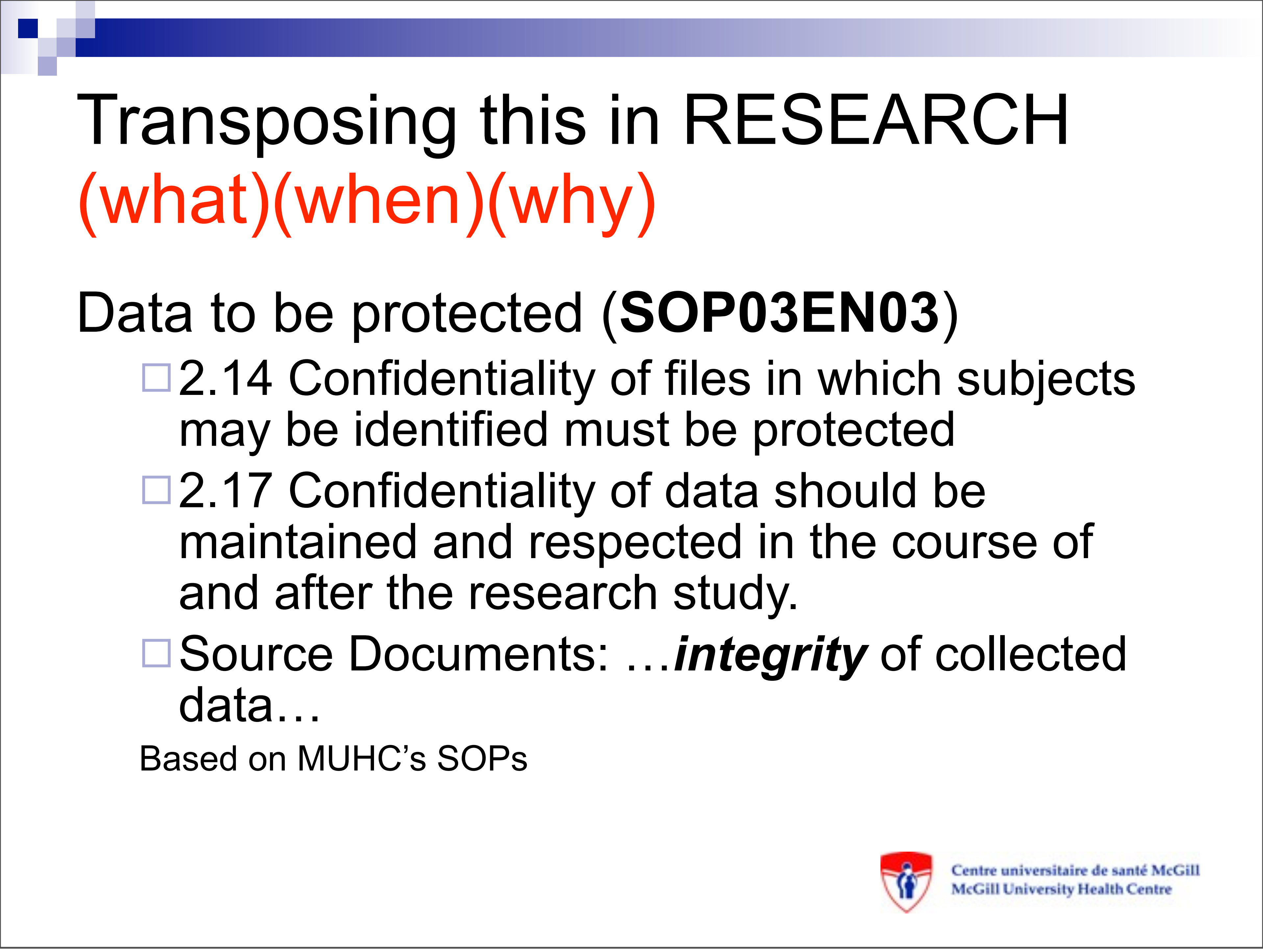
To complete the installation of the HSM, you need access to physical lock keys & chip cards. The physical keys will give access to a component inside the HSM that can read the smartcard. The latter serves as a configuration tool & a transport mechanism for the various MFK components. Yes, even the MFK is divided in multiple components (on average 2-3) each the responsibility of a key custodian. Once the installation is done, the unit can go into the running state. Today, FIs (Financial Institutions) usually configure & install the box remotely with some other secure tools.

Running State:

The HSM is used to process transactions, protect databases, generate working keys for other functions…

Terminated State:

The HSM has to go back to a factory state before the unit can be shipped outside the institution. All MFK key components need to be known for reinjection in another HSM.



Transposing this in RESEARCH (what)(when)(why)

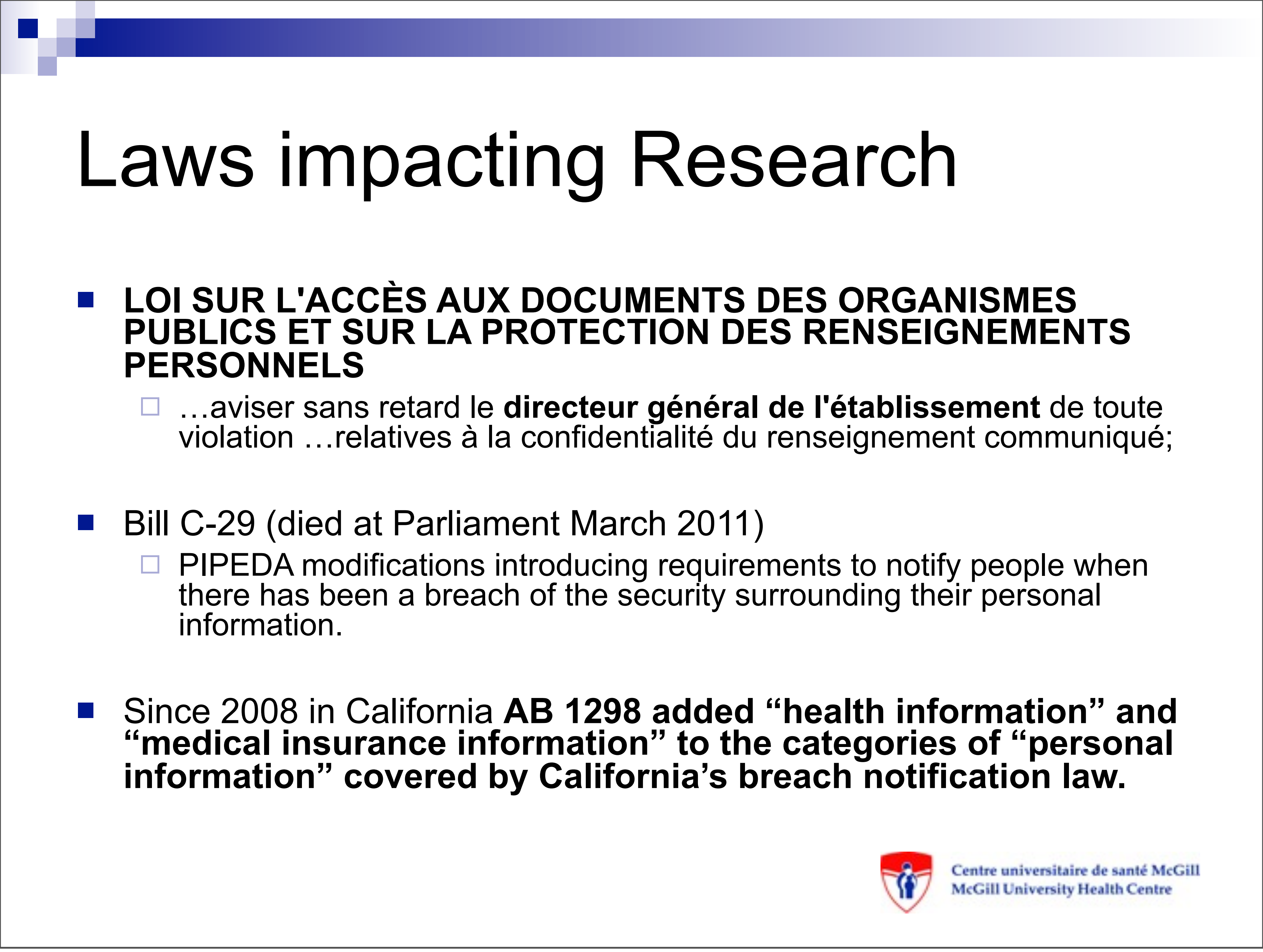
Data to be protected (**SOP03EN03**)

- □ 2.14 Confidentiality of files in which subjects may be identified must be protected
- □ 2.17 Confidentiality of data should be maintained and respected in the course of and after the research study.
- □ Source Documents: …***integrity*** of collected data…

Based on MUHC's SOPs

Research SOPs from MUHC were revised in OCTOBER 2010

On the MUHC intranet we can find the previous version (2008).



Laws impacting Research

- **LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**
  - …aviser sans retard le **directeur général de l'établissement** de toute violation …relatives à la confidentialité du renseignement communiqué;
- Bill C-29 (died at Parliament March 2011)
  - PIPEDA modifications introducing requirements to notify people when there has been a breach of the security surrounding their personal information.
- Since 2008 in California **AB 1298 added “health information” and “medical insurance information” to the categories of “personal information” covered by California’s breach notification law.**

Centre universitaire de santé McGill
McGill University Health Centre

Loi sur l’accès aux documents et organismes public…

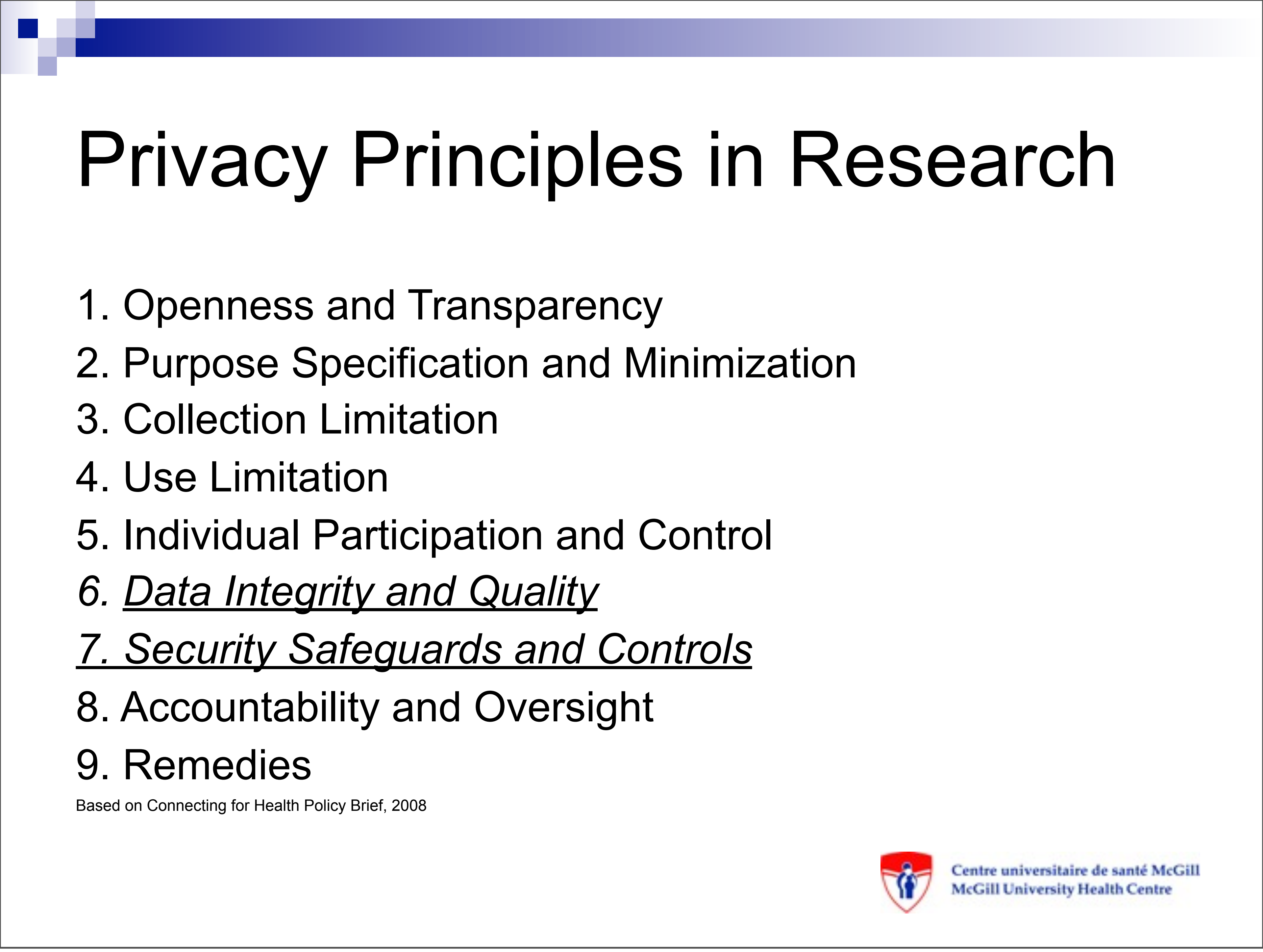
http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html

Bill C-29 (Pipeda: Personal Information Protection & Electronic Documents Act)

http://www2.parl.gc.ca/content/hoc/Bills/403/Government/C-29/C-29_1/C-29_1.PDF

California AB 1298

http://info.sen.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_cfa_20070905_200232_asm_floor.html



Privacy Principles in Research

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. *Data Integrity and Quality*
7. *Security Safeguards and Controls*
8. Accountability and Oversight
9. Remedies

Based on Connecting for Health Policy Brief, 2008

Centre universitaire de santé McGill
McGill University Health Centre

Tri-council Policy Statement (CRSH, CRSNG et IRSC) 2010:

They say just about the same thing concerning Safeguarding Information in Chap5 on Privacy & Confidentiality

(a) the type of information to be collected;

(b) the purpose for which the information will be used, and the purpose of any secondary use of identifiable information;

(c) limits on the use, disclosure and retention of the information;

(d) risks to participants should the security of the data be breached, including risks of re-identification of individuals;

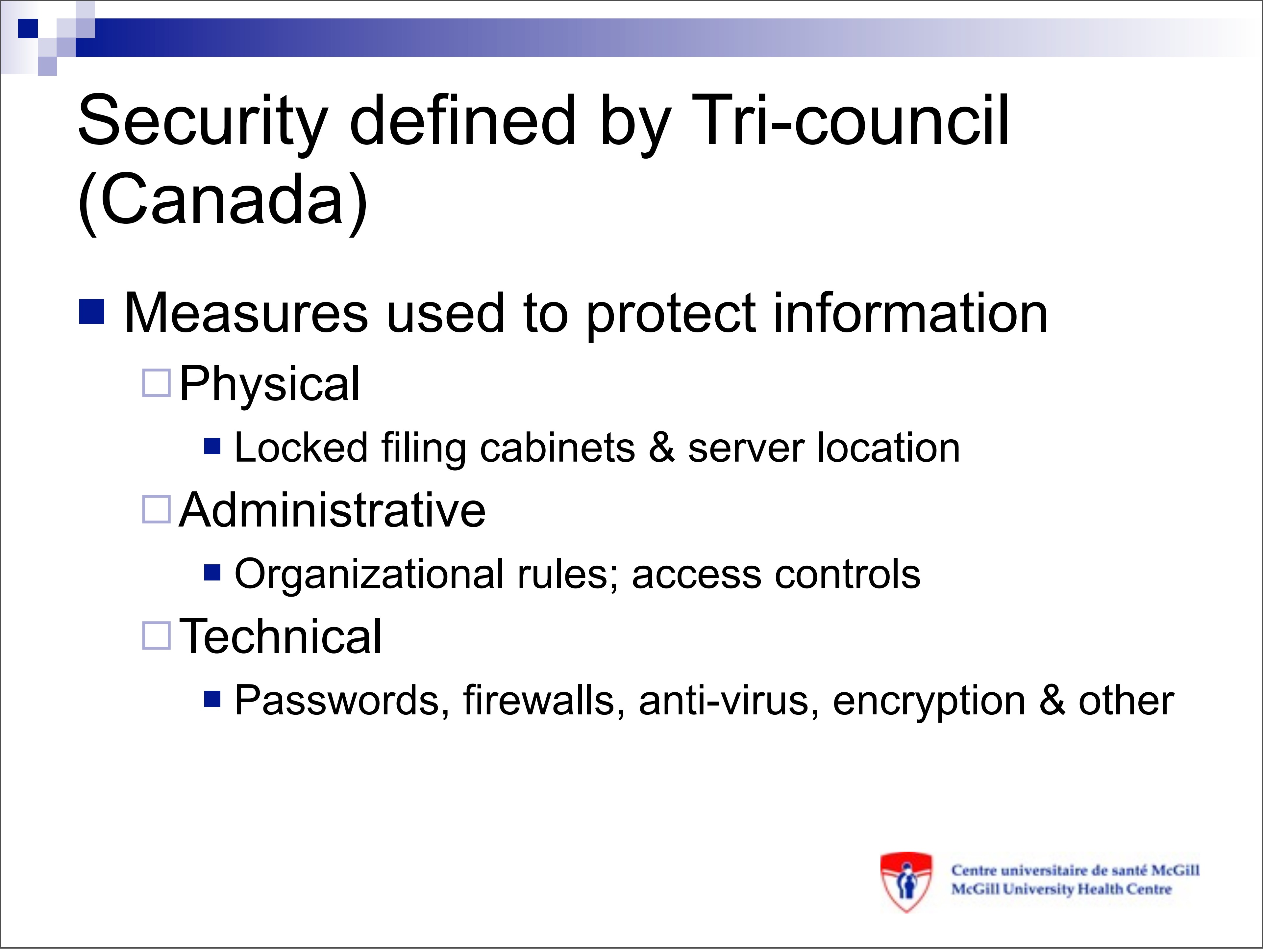
(e) appropriate security safeguards for the full life cycle of information;

(f) any recording of observations (e.g., photographs, videos, sound recordings) in the research that may allow identification of particular participants;

(g) any anticipated uses of personal information from the research; and

(h) any anticipated linkage of data gathered in the research with other data about participants, whether those data are contained in public or personal records

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, December 2010.



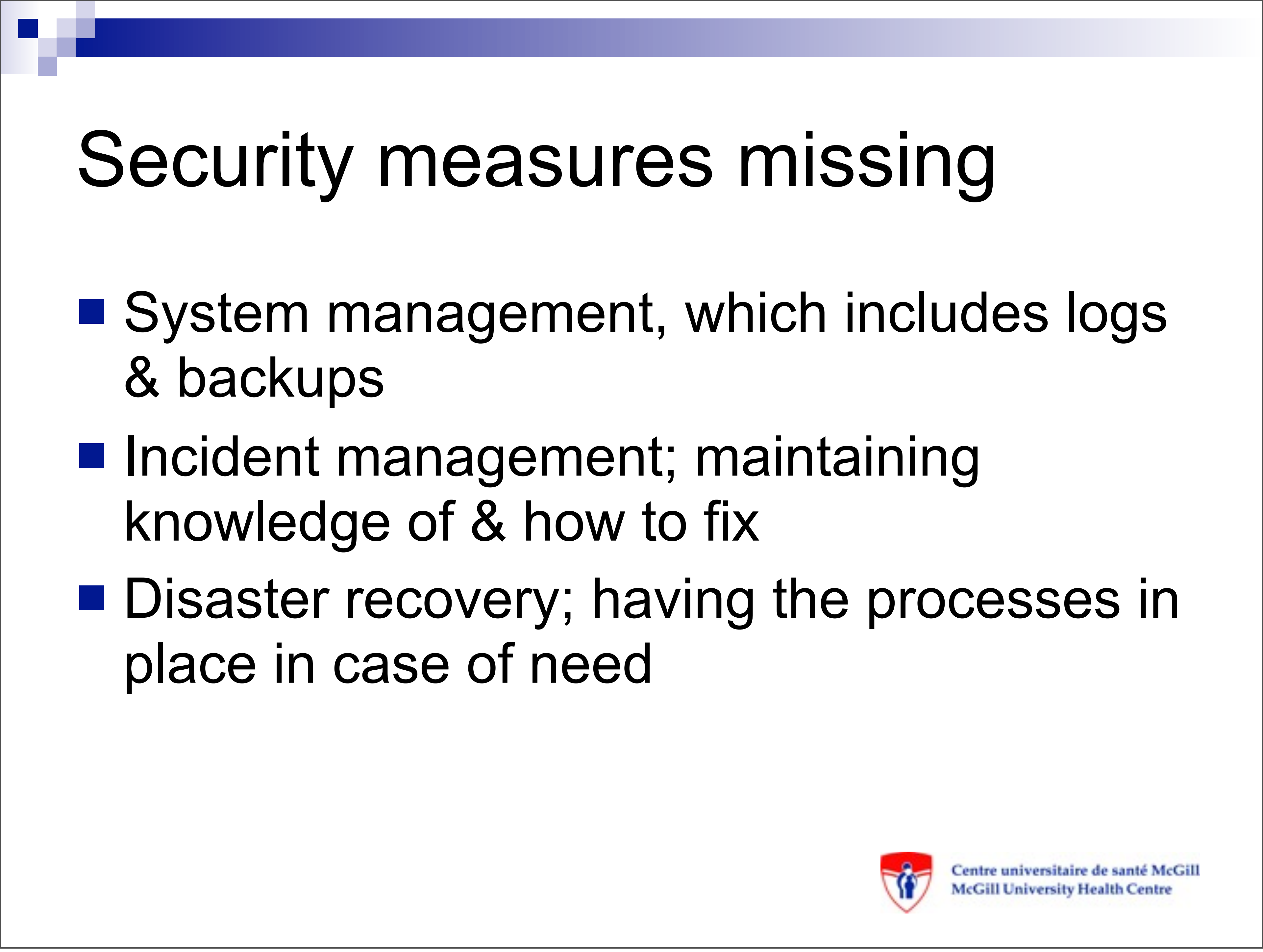
Security defined by Tri-council (Canada)

- Measures used to protect information
  - □ Physical
    - Locked filing cabinets & server location
  - □ Administrative
    - Organizational rules; access controls
  - □ Technical
    - Passwords, firewalls, anti-virus, encryption & other

Centre universitaire de santé McGill
McGill University Health Centre

Security

Security refers to measures used to protect information. It includes physical, administrative and technical safeguards. An individual or organization fulfils its confidentiality duties, in part, by adopting and enforcing appropriate security measures. Physical safeguards include the use of locked filing cabinets, and the location of computers containing research data away from public areas. Administrative safeguards include the development and enforcement of organizational rules about who has access to personal information about participants. Technical safeguards include use of computer passwords, firewalls, anti-virus software, encryption and other measures that protect data from unauthorized access, loss or modification.



Security measures missing

- System management, which includes logs & backups
- Incident management; maintaining knowledge of & how to fix
- Disaster recovery; having the processes in place in case of need

Centre universitaire de santé McGill
McGill University Health Centre

It is not because these subjects are not covered within the Ethical Research documentation that they are of no importance within the context of a research project. These security aspects need to be accounted for, whether or not by the research team or the IT entity supporting the research project. However, we won't cover any of these elements during this talk.

LOG management for example are essential in maintaining the integrity of the research data. Any data modification is logged on the system & normally these should be daily extracted from the server to be analyzed by specialized security monitoring technologies. If this isn't possible, the logs have to be protected from modifications. The ability to recover from a system failure, hardware of software is an essential aspect of availability (CIA triad). To avoid any repetition of system malfunctions; a register of incidents & measures taken to fix them is a necessity. Again, this could be part of a larger process taken in charge by a IT research entity.

U.S. Department of Health & Human Services (HHS.gov)

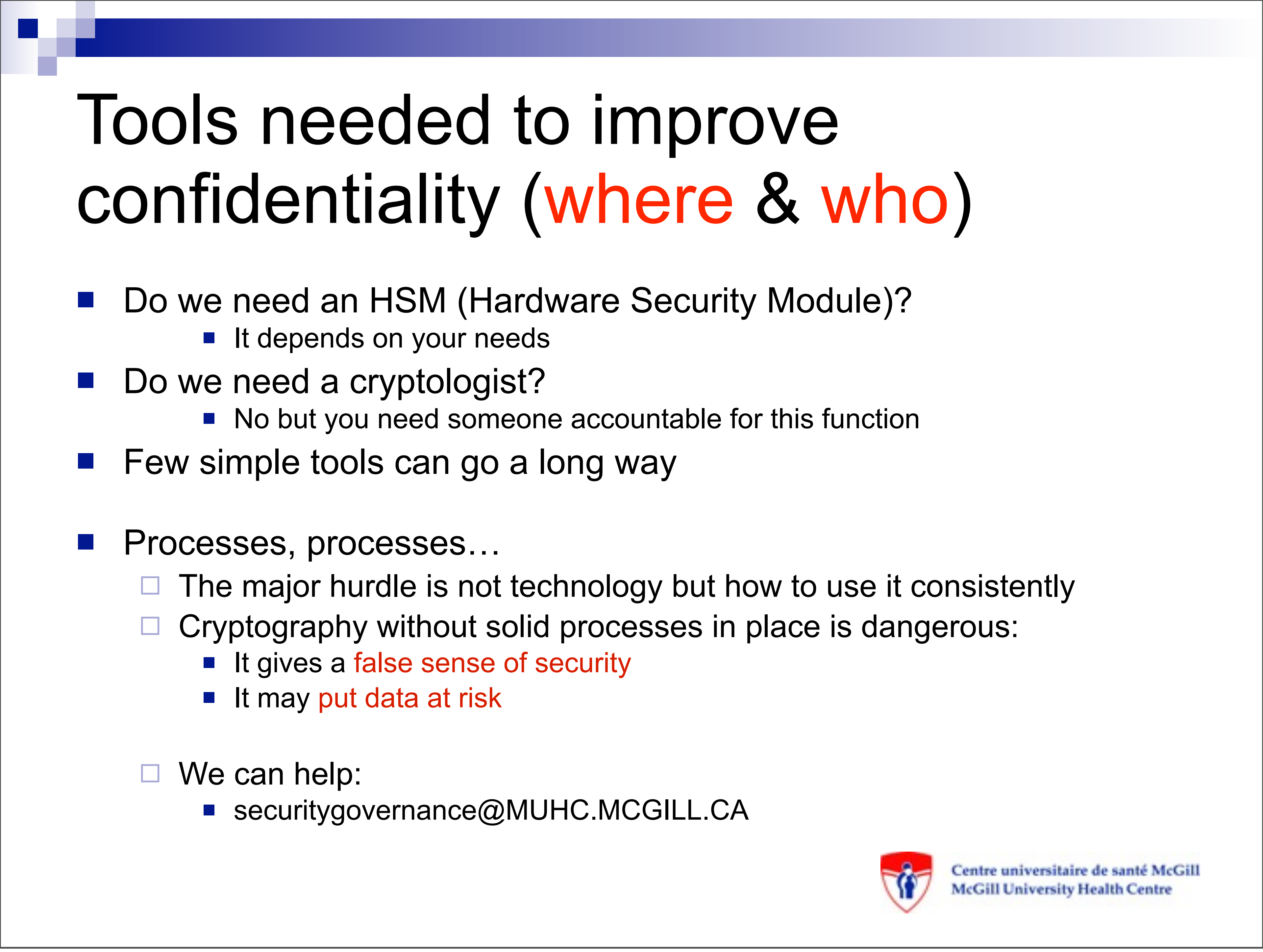
Institutional Review Board Guidebook

Chapter 3.D

the medical care provider maintaining the record:
(iv) requires that adequate safeguards to protect the record or information from unauthorized disclosure be established and maintained by the user or recipient, including a program for removal or destruction of identifiers; In section 3.E:

5. Does the institution have a data and safety monitoring board? If so, should it be asked to monitor the project under review? If the institution does not have a data and safety monitoring board, should the IRB request or recommend that one be appointed, either by the institution or the sponsor, for this project?

http://www.hhs.gov/ohrp/archive/irb/irb_chapter3.htm#e5



Tools needed to improve confidentiality (where & who)

- Do we need an HSM (Hardware Security Module)?
    - It depends on your needs
- Do we need a cryptologist?
    - No but you need someone accountable for this function
- Few simple tools can go a long way

- Processes, processes…
    - □ The major hurdle is not technology but how to use it consistently
    - □ Cryptography without solid processes in place is dangerous:
        - It gives a false sense of security
        - It may put data at risk

    - □ We can help:
        - securitygovernance@MUHC.MCGILL.CA

Centre universitaire de santé McGill
McGill University Health Centre

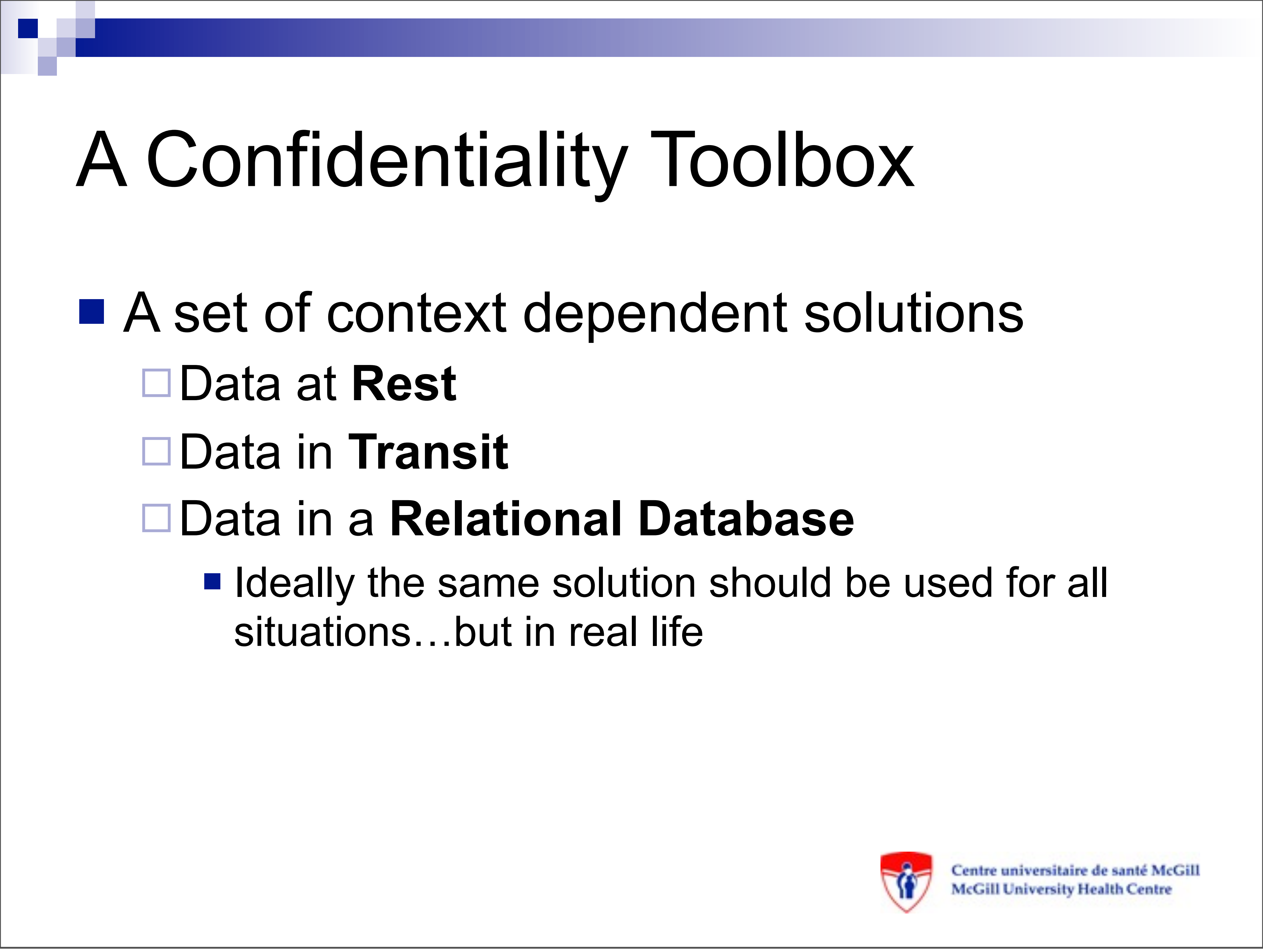
Without a better understanding of what currently exist within research projects, I am forced to evaluate what exists based on my personal experience of 11 months here at the MUHC.

From what I have seen IT process maturity is not at par with IT in the private sector. And the gap is even wider when you compare our IT infrastructure with those in the Financial Industry. We have to understand that for FIs, IT is their bread & butter. In Health & Health research we are still pretty much relying on paper.

Patient charts are paper based except for a few clinical systems capable of storing information. Note that more & more crucial & important information is being stored in databanks today than a few years ago. Yet we are still at the start of this trend. But it is normal that there is an increase need in IT processes & IT security processes. Access controls are very important in these situations.

Security oriented services are not part of a catalogue that you can pick & choose according to your needs.

The confidentiality Toolbox is the first set of tools & processes that you can use to implement security requirements within your research project.



A Confidentiality Toolbox

- A set of context dependent solutions
  - □ Data at **Rest**
  - □ Data in **Transit**
  - □ Data in a **Relational Database**
    - Ideally the same solution should be used for all situations…but in real life

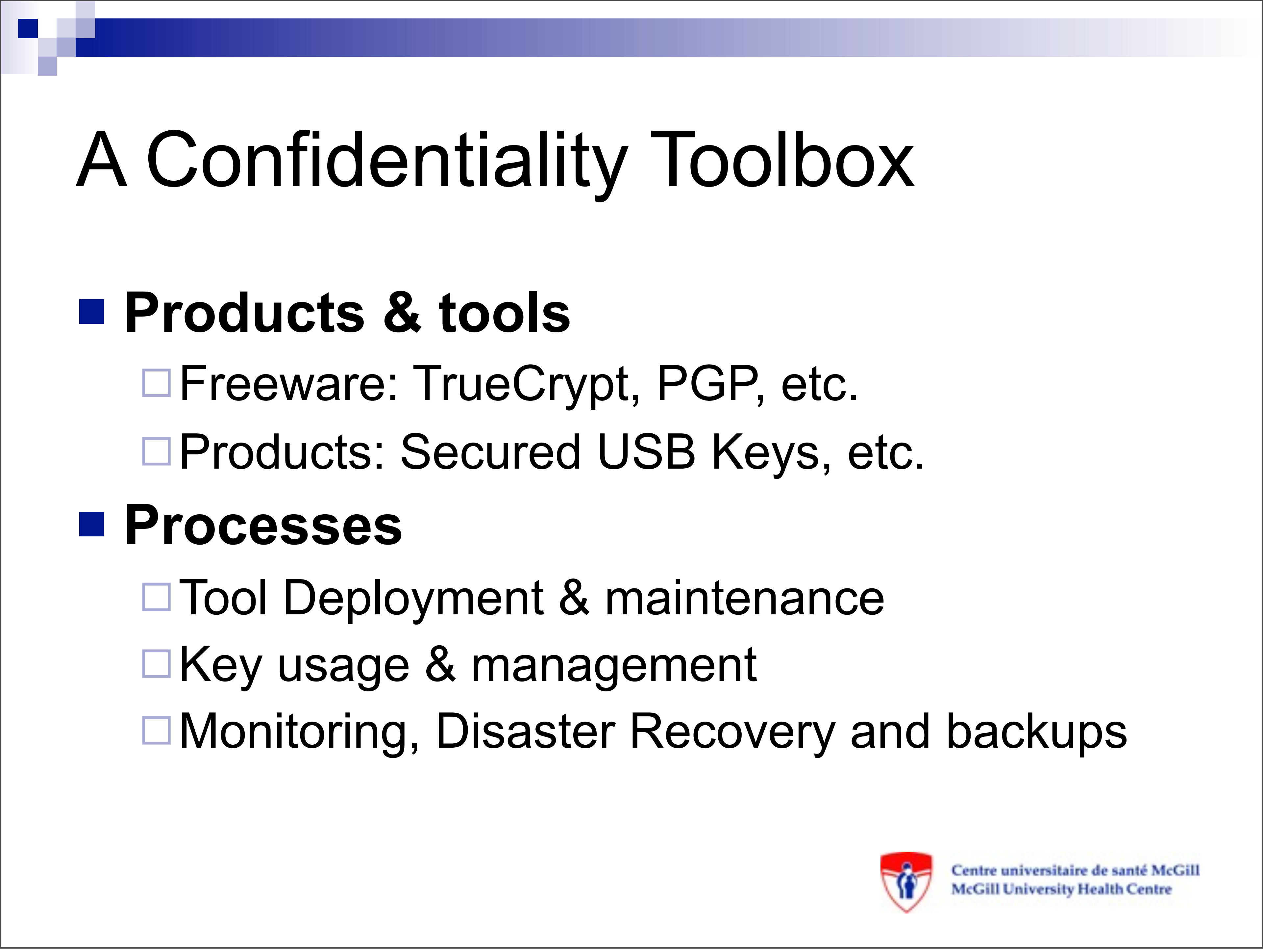
Centre universitaire de santé McGill
McGill University Health Centre

We have to distinguish between various context in relation to the logical information you are trying to protect.

We will provide you with these toolbox in the very near future; They will represent recipes to be used given the sensibility of the information to manipulate and the context of that manipulation.

For those who wish to move forward right away, we will provide you with the needed assistance to do so.

In the mean time, we will look at how to do these simple tasks with the security umbrella.



A Confidentiality Toolbox

- **Products & tools**
  - □ Freeware: TrueCrypt, PGP, etc.
  - □ Products: Secured USB Keys, etc.
- **Processes**
  - □ Tool Deployment & maintenance
  - □ Key usage & management
  - □ Monitoring, Disaster Recovery and backups

Centre universitaire de santé McGill
McGill University Health Centre

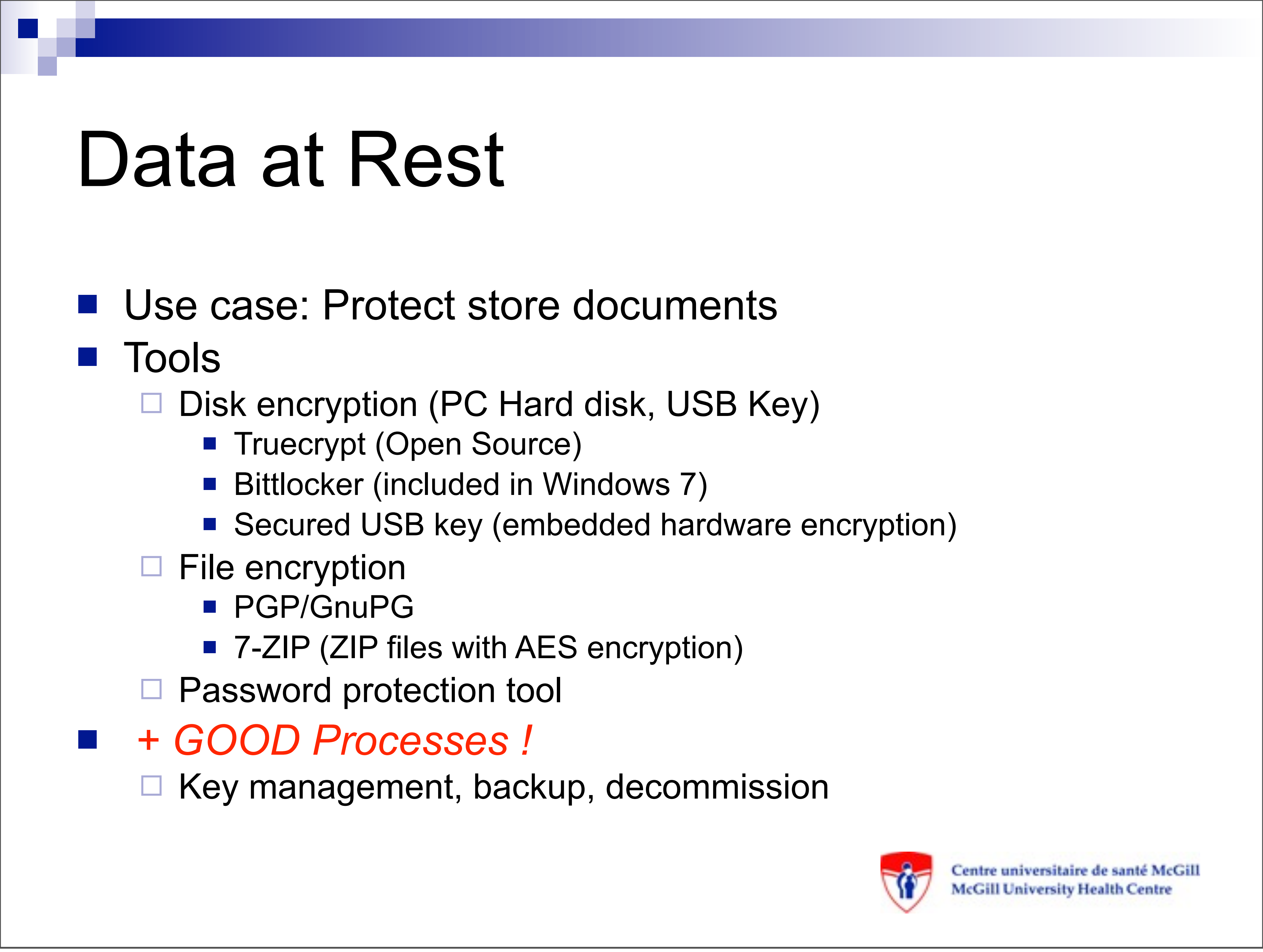
These are the elements needed in the Crypto Toolbox;

First we have to define the roles that are needed to ensure that a crypto implementation is adequate & cannot be undone because of an error in implementation.

Users roles are a necessity because there is a need to safeguard secret components between various individuals. Even within Financial Institutions; some people know a portion of a secret. It is expected that no collusion is possible.

Products to acquire range from close to 0$ for Freeware/Shareware, moving on to 50$ for a secured USB key to many $Ks for host based hardware security modules. Most database vendors offer cryptography within their products, it is then a question of making sure we are implementing this function the correct way.

Just like individual roles are needed to define; proper processes are needed to ensure everyone implements “security” the same way. The idea is to simplify security to a recipe. We don’t need to know how a motor works to drive a car, but we do need to know what to do to start the motor & put gas in the thank.



Data at Rest

- Use case: Protect store documents
- Tools
  - Disk encryption (PC Hard disk, USB Key)
    - Truecrypt (Open Source)
    - Bittlocker (included in Windows 7)
    - Secured USB key (embedded hardware encryption)
  - File encryption
    - PGP/GnuPG
    - 7-ZIP (ZIP files with AES encryption)
  - Password protection tool
- *+ GOOD Processes !*
  - Key management, backup, decommission

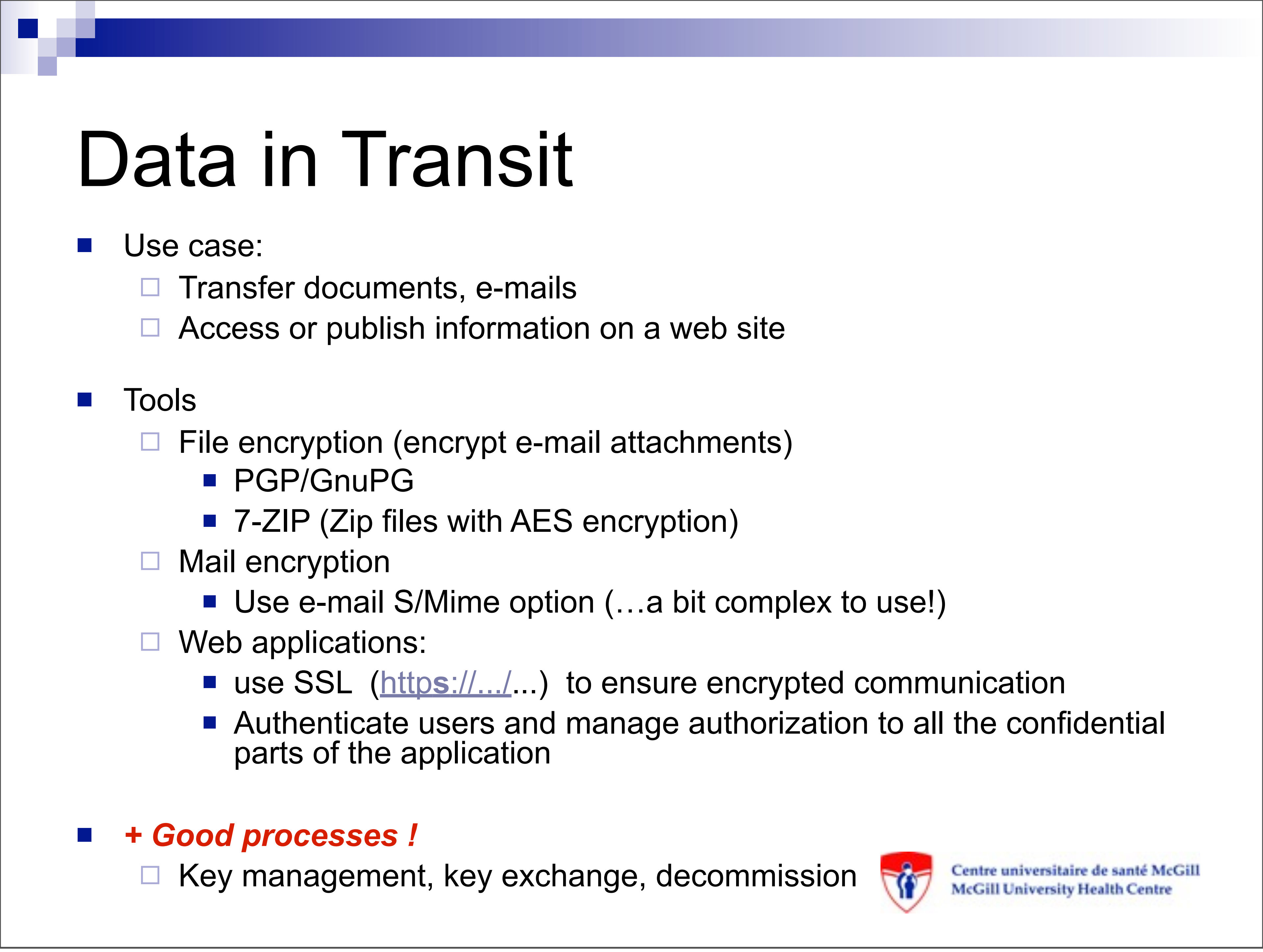
Centre universitaire de santé McGill
McGill University Health Centre

Most research projects are no longer paper based like they were a few years ago.

A lot of data pertaining to the protocol is needed to ensure that the research is adequate, can continue on its path & status reports are instantly available.

Those pieces of information need to be conserved in their format for years to go (***from 5 years up to 25 years after the research is finished***). *Règlement sur les aliments et drogues*, C.R.C., c. 870. *Règlement modifiant le Règlement sur les aliments et drogues* (1024 – essais cliniques), (2001) 135 Gazette du Canada partie **II**, 1116-1153 (SOR/DORS/2001-203). En ligne. <http://lois.justice.gc.ca/fr/F-27/C.R.C.-ch.870/index.html >. Consulté le 31 août 2006.

For data at rest the important element is being able to retrieve the information once everyone that worked on the project are no longer there. Being able to retrieve the information once it is encrypted is not possible unless there are proper processes in place to obtain the passwords/key components/secrets that were used to implement the security architecture.



Data in Transit

- Use case:
  - Transfer documents, e-mails
  - Access or publish information on a web site
- Tools
  - File encryption (encrypt e-mail attachments)
    - PGP/GnuPG
    - 7-ZIP (Zip files with AES encryption)
  - Mail encryption
    - Use e-mail S/Mime option (…a bit complex to use!)
  - Web applications:
    - use SSL (https://.../...) to ensure encrypted communication
    - Authenticate users and manage authorization to all the confidential parts of the application
- ***+ Good processes !***
  - Key management, key exchange, decommission

Centre universitaire de santé McGill
McGill University Health Centre

There is no research done in isolation from the rest of the world. Money for the research comes from outside entities. Data needs to be transported & shared with other research centers, etc.

The ability to transfer large amount of information & to do it in a secure fashion, without wondering if this could impact the finality of the research or breach patient's confidentiality is important.

There are many methods available & we won't go thru them in this talk, but the Toolkit will contain instructions on the most popular with the pros & cons for each one.

Normally there is a sense of temporality in data that is transferred. Once the transfer is completed, this data is no longer needed & the format under which it was put is destroyed to ensure that it no longer exists outside the database (which includes secured access & data protection).

Data in a DataBase

- Administrator access control is paramount
- Select a database that will allow the use of encryption like TDE for Microsoft & Oracle
  - □ Or look for an alternative that offers the same
- Key management becomes important
  - □ Keys stored in software (instead of hardware) aren’t really secured
    - Oracle (key) Wallet= manual start with split-password: possible software solution
- TDE: Transparent Data Encryption

Centre universitaire de santé McGill
McGill University Health Centre

Christian Kirsch -The role of encryption in database security, Thales, 2009:

Place key management at the core of your IT security infrastructure
Store keys in hardware, rather than software,
Mirror your paper-based security policies in the hardware to pass audits with ease,
Use strong authentication techniques for your administrators,
Ensure different administrators control access to encrypted data to those responsible for access to keys,
Automate your key management tasks,
Ensure keys are easy to locate by consolidating keys in one system,
Keep an audit trail of your key management activities,
http://www.net-security.org/article.php?id=1232&p=1

Mot de la Fin

- An opportunity exits in Health Research to leverage IT Security as a “business” enabler
- As management consultant Peter Drucker once said: “If you can’t measure it, you can’t manage it.”
- Our number: securitygovernance@MUHC.MCGILL.CA

Centre universitaire de santé McGill
McGill University Health Centre

I’d like to thank everyone for your attendance today. I hope that I didn’t scare to many researches with these security concepts.

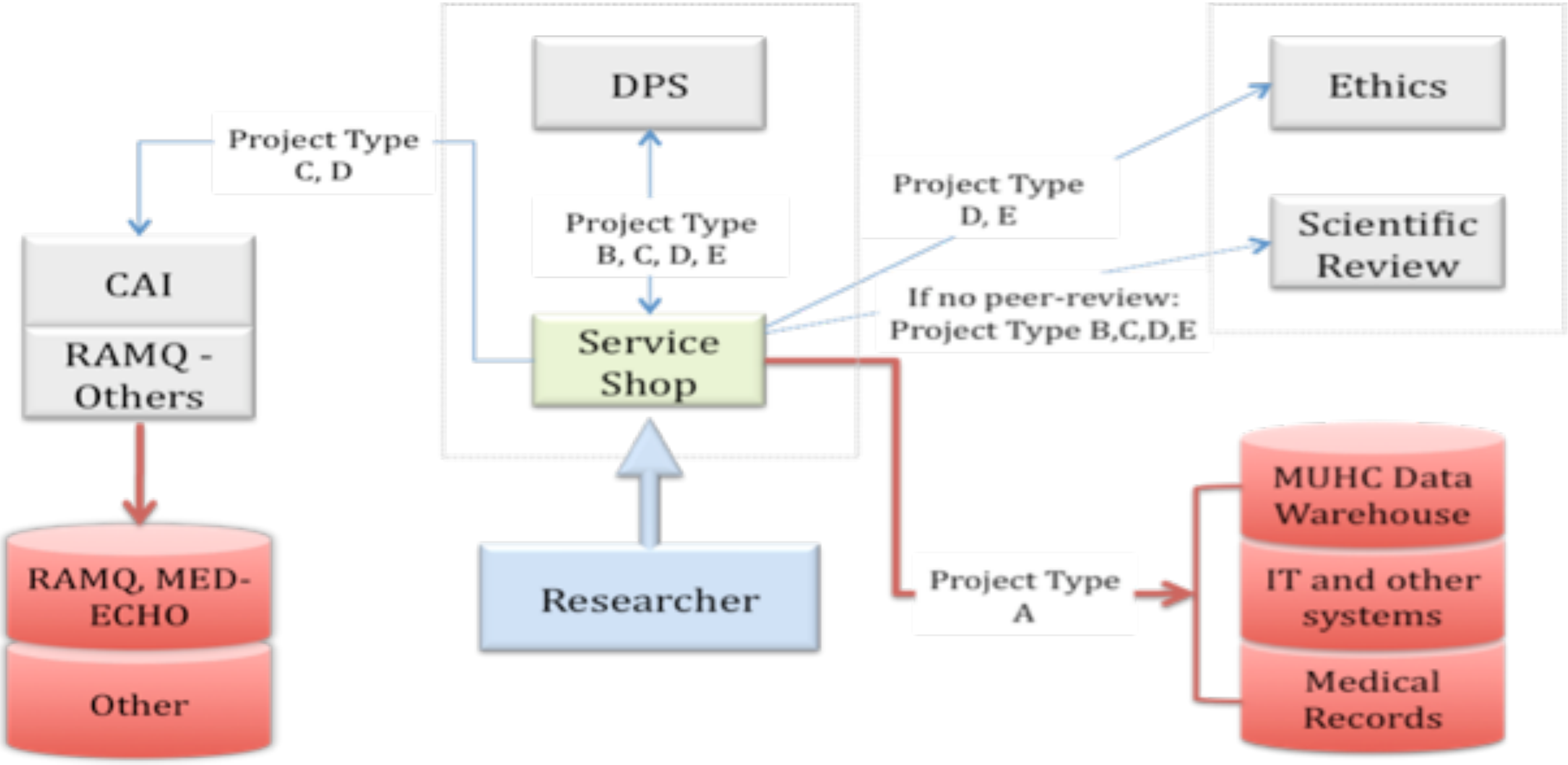
We are available to help you implement these security requirements within your protocol.

So don’t hesitate to reach us. It will be a pleasure for us to assist you in this task.

APPENDIX

Centre universitaire de santé McGill
McGill University Health Centre

Proposed MUHC DATA SERVICE SHOP



Centre universitaire de santé McGill
McGill University Health Centre

This drawing was extracted from a research project that was put forward a few years ago but it didn’t go thru for reasons that I don’t have.

It is clear however that in the very near future (2014 or before) that we will need to implement such a setup to facilitate access to medical information if we are to attract & maintain quality researchers here at McGill.

There are many professions involved in the Hospital & Health research context. Each one have their own set of responsibilities & point of views & each one are consulted before anything can change.

Having a set of tools available for researchers is a step in the right direction.

LIST OF ACRONYMS AND ABBREVIATIONS

- CAREB Canadian Association of Research Ethics Boards
- CIHR Canadian Institutes of Health Research
- IIWG Initial Implementation Working Group
- NCEHR National Council on Ethics in Human Research
- NSERC Natural Sciences and Engineering Research Council of Canada
- PBPs document CIHR Privacy Best Practices document. Full title: CIHR Best Practices for Protecting Privacy in Health Research (September, 2005)
- PRE Interagency Advisory Panel on Research Ethics
- RMGA Quebec Network of Applied Genetic Medicine
- REB Research ethics board
- SRE Secretariat on Research Ethics
- SSHRC Social Sciences and Humanities Research Council of Canada
- SSHSWC Social Sciences and Humanities Research Ethics Special Working Committee
- Tri-Agency Tri-Council: Pertaining to these three federal research agencies: Canadian
  - Institutes of Health Research, Social Sciences and Humanities
  - Research Council of Canada, and the Natural Sciences and
  - Engineering Research Council of Canada

Centre universitaire de santé McGill
McGill University Health Centre

LIST OF ACRONYMS AND ABBREVIATIONS (security)

- AES: Advance Encryption Standard; the most recent algo crypto to arrive on the market (symmetrical)
- Asymmetrical; In reference to a crypto algo; a different key is used for scrambling the information & to extract the clear data from the cryptogram (example: RSA, ECC)
- Cryptogram: The end result of data encrypted, could also be a reference to a crypto key protected by the MFK
- DES: Data Encryption Standard; the first commercial crypto algo; 3DES is a variation still used extensively in Banks (symmetrical)
- ECC: Elliptic Curve Cryptology, invented here in Canada (Waterlo); a crypto algo used a lot in cell phones (asymmetrical)
- Hashing: The transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string; (MD4, MD5, SHA-1, SHA-2); in cryptology this is used extensively in electronic signature standards; integrity functions
- KEK: Key Exchange Key; is a key used to establish a secured link between to entities who want to exchange confidential information
- MAC: Message authentication code; a mechanism used for information integrity
- MFK: Master File Key; The key responsible for the protection of all the other keys
- PGP: Pretty Good Privacy; The first crypto application for everyone; today available for free (personal usage) & even for the enterprise
- RSA: Rivest, Shamir & Aldeman; named after the 3 who managed to get a patent for mathematical properties of prime numbers; and turned this into a crypto algo (asymmetrical)