




# BHF Southern African Conference





*Navigating the complexities of the new legislative framework*

Peter Hill, Director: IT Governance Network

- ❖ The practical implementation of the PPI Act
- ❖ Challenges and changes to the way medical schemes are to be administered
- ❖ The role and function of the Information Protection Officer
- ❖ Who is the “Responsible Party” and what are their obligations under the PPI Act?
- ❖ Why a Code of Conduct (for protecting personal information) within medical schemes would be a good idea?

## **The IT Governance Network (South Africa, US, UK, Switzerland)**

- ❖ Global leaders in IT Governance – 15 years experience
- ❖ International Privacy Expertise – 15 years experience
- ❖ Active participants at Parliamentary meetings finalising the Privacy legislation

## **Key People**

- ❖ Peter Hill, CISM, CISA, CGEIT, international IT governance specialist
- ❖ Michael Erner, lawyer, accredited Privacy Expert, “Independent Centre for Privacy Protection Schleswig-Holstein”, Germany

## **Significant clients**

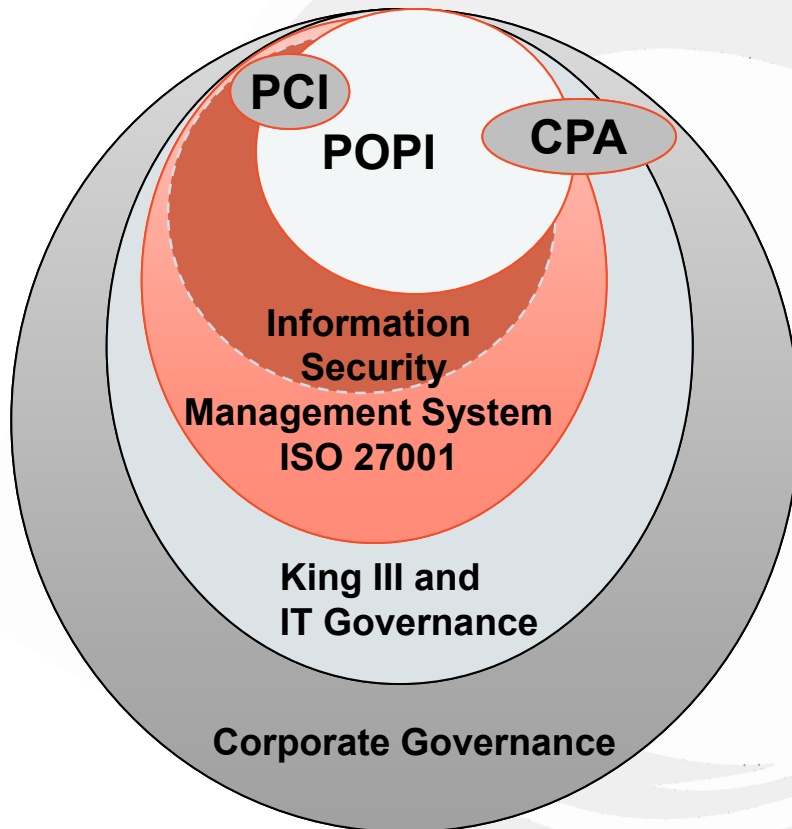
- ❖ Local banking, financial and retail institutions
- ❖ NASA
- ❖ Deutsche Telecom –global
- ❖ UBS

## **What we do**

- ❖ Consulting, Education, Privacy management solutions
- ❖ Independent external Information Protection Officers



# OVERLAP OF KING III, CPA, POPI AND PCI



## Consumer Protection Act (CPA)

### Protection against discriminatory marketing

8. A supplier **must not directly or indirectly treat any person differently than any other**, in a manner that constitutes unfair discrimination on one or more grounds set out in section 9 of the Constitution, or one or more grounds set out in Chapter 2 of the Promotion of Equality and Prevention of Unfair Discrimination Act, when determining whether to report, or reporting, any personal information of such person.

### Prohibited transactions, agreements, terms or conditions

51. (1) A supplier **must not make** a transaction or agreement subject to any term or condition if it expresses an agreement by the consumer to—provide a personal identification code or number to be used to access an account.

51. (2) A supplier **may not request** or demand a consumer to reveal any personal identification code.

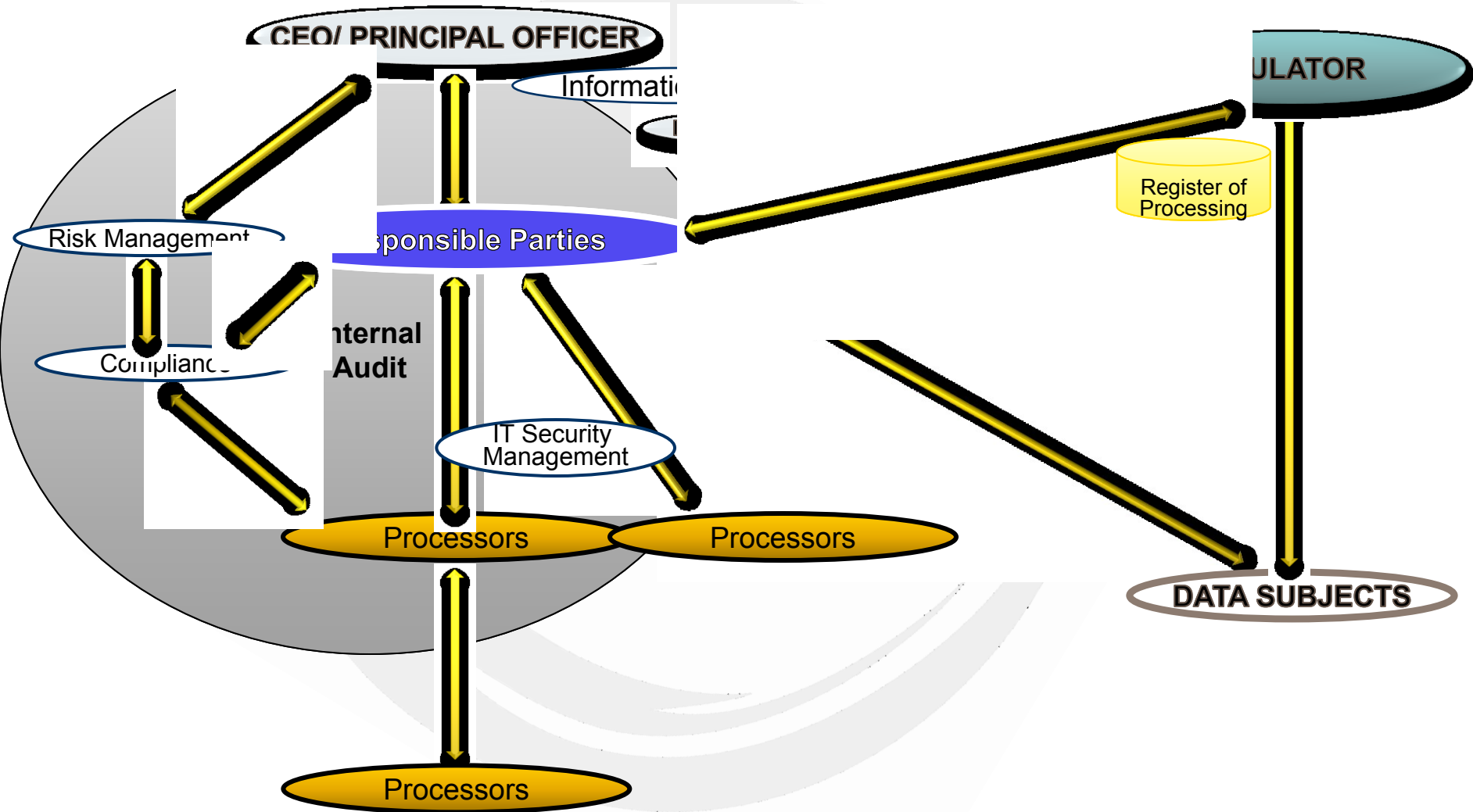
(4) This section **does not preclude** a supplier to require a personal identification code or number in order to facilitate a transaction that in the normal course of business necessitates the provision of such code or number.

- ❖ Ignorant of Individuals' constitutional right to Privacy
- ❖ Impact on Reputation leading to loss of business
- ❖ Cost of adjusting existing business processes
- ❖ Cost of additional security (confidentiality, integrity, availability)
- ❖ Poor record management increases cost of searching for, protecting and deleting personal information
- ❖ Civil litigation – cost and damages awarded
- ❖ Regulator audits, costly investigations
- ❖ Criminal offences leading to Penalties

# THE KEY ROLES FOR PPI

- ❖ The Regulator
- ❖ Data Subjects
- ❖ Responsible Parties
- ❖ Processors
- ❖ Information Officers
- ❖ Information Protection Officers
  
- ❖ Risk Managers
- ❖ Information Security Managers
- ❖ Compliance Officers

# THE KEY ROLES FOR PPI



# THE ROLE OF RESPONSIBLE PARTIES

18. (1) A **responsible party must secure the integrity** of personal information in its possession or under its control by taking appropriate, reasonable **technical and organisational measures** to prevent—
- (a) loss of, damage to or unauthorised destruction of personal information; and;
  - (b) unlawful access to or processing of personal information.
- (2) In order to give effect to subsection (1), the **responsible party must take reasonable measures** to—
- (a) *identify all reasonably foreseeable internal and external **risks** to personal information in its possession or under its control;*
  - (b) *establish and maintain appropriate **safeguards** against the risks identified;*
  - (c) *regularly verify that the safeguards are **effectively implemented**; and ensure that the safeguards are **continually updated** in response to new risks or deficiencies in previously implemented safeguards.*
- (3) The responsible party must have due regard to **generally accepted information security practices** and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

# NOTIFICATION OF PROCESSING

50. (1) A responsible party must **notify the Regulator before commencing** the —
- (a) fully or partly automated processing of personal information or categories of personal information intended to serve a single purpose or different related purposes; or
  - (b) non-automated processing of personal information intended to serve a single purpose or different related purposes, if such processing is subject to a prior investigation.
- (2) The notification referred to in subsection (1) must be noted in a register kept by the Regulator for this purpose.

## Notification to contain specific particulars

- 51.(1) The notification must contain the following particulars:
- (a) The **name** and **address** of the responsible party;
  - (b) the **purpose** of the processing;
  - (c) a **description of the categories of data subjects** and of the information or categories of information relating thereto;
  - (d) the **recipients** or categories of recipients to whom the personal information may be supplied;
  - (e) **planned trans-border flows** of personal information; and
  - (f) a general description allowing a preliminary assessment of the suitability of the **information security measures to be implemented** by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

## Notification of security compromises

21. (1) Where there are reasonable grounds to believe that the personal information of a data subject has been **accessed or acquired by any unauthorised person**, the responsible party, or any third party processing personal information under the authority of a responsible party, **must notify** the—
- (a) Regulator; and*
  - (b) data subject, unless the identity of such data subject cannot be established.*
- (2) The notification referred to in subsection (1) must be made **as soon as reasonably possible after the discovery** of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.
- (3) The responsible party may only delay notification of the data subject if the South African Police Service, the National Intelligence Agency or the Regulator determines that notification will impede a criminal investigation.

## Principle 1 - Accountability

- ❖ The **responsible party** must ensure that the conditions set out in the Act, and all the measures required, are complied with.
  - “responsible party” means a public or private body or any other person which, *alone or in conjunction with others, determines the purpose of and means for processing personal information;*

## Principle 2 - Processing limitation

- ❖ Business processes provide the context for processing personal information – i.e. the specific purpose
- ❖ Data collection must be proportionate to purpose – **minimal**
- ❖ Data processing must be for a **legitimate purpose**
- ❖ Data subject must give **consent**
- ❖ Collection of personal data must be **directly** from the data subject unless it is contained in a public record
- ❖ Data models prevent inference of prohibited data elements
- ❖ **Limit the transfer** of personal data to service providers
- ❖ Data subject must be able to object, in prescribed manner.

## Principle 3 - Purpose specification

- ❖ Collection of personal information must be for a **specifically defined**, lawful purpose related to a function of the responsible party
- ❖ Data subject must be **aware** of the purpose of collecting data
- ❖ The **purpose** for processing personal information must be clear
- ❖ **Record retention** must not be longer than necessary unless required by law, a contract or the data subject has consented
- ❖ A record of the use of personal data to make a decision must be retained for such period required by a law or **long enough** for the data subject to request access to the record
- ❖ **Destroy**, delete or de-indentify as soon as practically possible
- ❖ Destruction of personal information must be in a manner that prevents reconstruction in an intelligible form.

## **Principle 4 - Further processing limitation**

- ❖ Further processing must be compatible with original purpose
- ❖ Be aware of the potential consequences of further processing
- ❖ Take note of any contractual rights and obligations
- ❖ Take steps to prevent further processing of personal data
- ❖ Data mining must not exceed original purpose
- ❖ Allow retention for historical, statistical or research purposes
- ❖ Stop unlawful processing.

## Principle 5 - Information quality

- ❖ Maintain the accuracy of collected personal information
- ❖ Check that personal data is not misleading
- ❖ Ensure that personal data is up-to-date
- ❖ Be aware of the impact the integrity of personal data has on the purpose for collecting personal data

Note: master data must exclude unnecessary records

Note: master data must be secured, and accessed only on the need-to-know basis.

## Principle 6 – Openness

- ❖ Only process personal data after notifying the Regulator
- ❖ The data subject must be aware of the collection of the data and the name and address of the responsible party, whether voluntary or mandatory, and of any law authorising collection, except if
  - ❖ data subject is already aware
  - ❖ all particulars are stated in PROATIA manual
  - ❖ data subject consents to non-compliance
  - ❖ information will be used without identifying data subject
  - ❖ Personal information is already in the public domain.

## **Principle 7 - Data subject participation**

- ❖ Establish communication processes with data subjects (via the Information Protection Officer)
- ❖ Provide data subjects with access to personal information
- ❖ Enable data subjects to request correction of personal data
- ❖ Manner of access to information is defined in PROATIA.

# HOW TO GET TO WHERE YOU NEED TO BE WITH PPI?



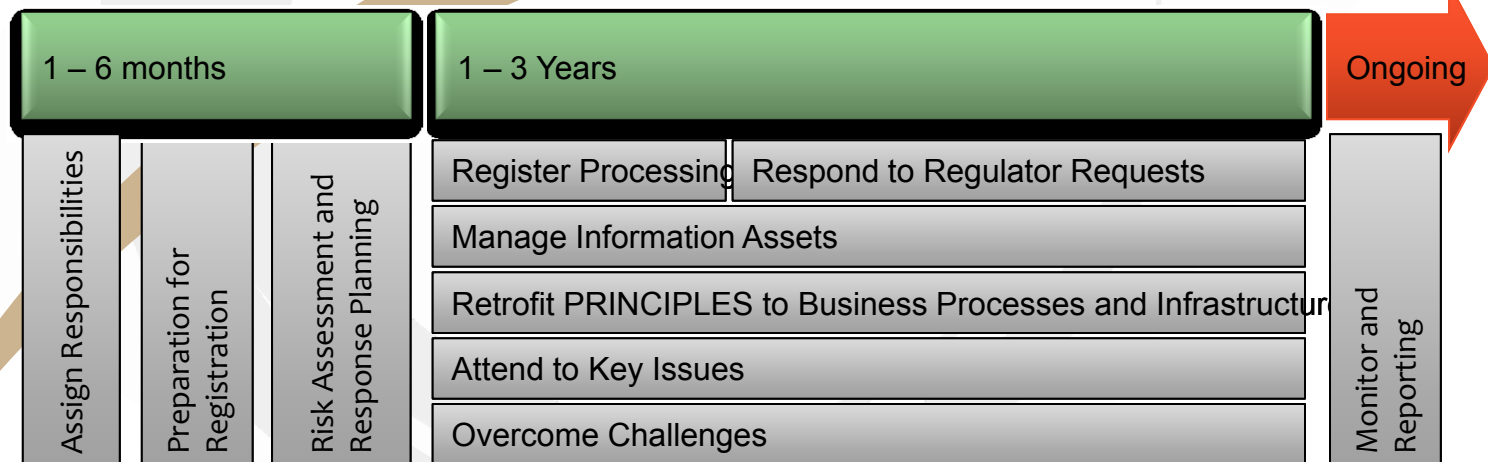
- ❖ Update current **Information Officer role** to include Information Protection Officer responsibilities, or delegate to deputy IPO
- ❖ **Identify** all Personal Information and the Responsible Parties
- ❖ **Identify** the Categories and Purpose for processing Personal Information
- ❖ **Prepare the forms** to register the Processing of Personal Information
- ❖ **Identify shortcomings** in compliance with the conditions for lawful processing
- ❖ **Identify risks** and risk responses
- ❖ **Take corrective action**
- ❖ **Notify the Regulator** of the categories and purpose of processing personal information

# EXAMPLES OF PERSONAL DATA

- ❖ General
- ❖ Special

- ❖ Retrofitting to existing processes and infrastructure
- ❖ Business purpose specific, proportionate to purpose
- ❖ Cease secondary and unlawful processing
- ❖ Internet-based processing
- ❖ Controlling third-parties
- ❖ Employee education
- ❖ Unstructured data
- ❖ Data destruction
- ❖ Data leakage
- ❖ Sustainability

# ROADMAP TO COMPLIANCE WITH PPI



# A CODE OF CONDUCT (FOR PROTECTING PERSONAL INFORMATION) WITHIN MEDICAL SCHEMES

- ❖ Not all schemes are staffed internally
- ❖ Often many administrative functions are outsourced
- ❖ A full-time information protection officer for each scheme could be costly
- ❖ Each scheme has many service providers (doctors, intermediaries, administrators, service providers to the administrators)
- ❖ Many schemes have the same relationships.

- ❖ Recent submissions by 3 major banks are just repeating previous submissions
- ❖ Chairman stressed companies that cannot demonstrate sufficient effort to date may not be eligible for an extension – if extensions are granted!
- ❖ Funding of regulator could be out of fees collected from companies registering late
- ❖ PPI Act is expected to be promulgated by December 2010



## QUESTIONS AND DISCUSSION

[www.personalprivacy.co.za](http://www.personalprivacy.co.za)

IT Governance Network  
South Africa, US, UK, Switzerland

PETER HILL  
+27 825588732  
+44 – (0)20 81333180  
+1 302-5044408  
[peter@itgovernance.com](mailto:peter@itgovernance.com)

 a meeting  
of minds  
The BHF Southern  
African Conference  
Sun City 22-25 August 2010

# HOW THE IT GOVERNANCE NETWORK CAN ASSIST?

## Guidance on:

- ❖ The Rights of Individuals
- ❖ Identifying Personal Information
- ❖ Identifying Responsible Parties
- ❖ Lawful and unlawful processing
- ❖ Processing Limitations
- ❖ Further Processing Limitations
- ❖ Contracting with Third Parties
- ❖ Notification to the Regulator
- ❖ The role and procedures of the Information Protection Officers

## Assistance with:

- ❖ Collection of Registration information
- ❖ Business process redesign
- ❖ Measures to enhance Confidentiality
- ❖ Measures to enhance Integrity
- ❖ Measures to enhance Availability
- ❖ Responding to Data Subject requests
- ❖ Working with the Regulator
- ❖ Conducting audits
- ❖ Independent Information Protection Office
- ❖ Drafting Code of Conduct

- ❖ Legal, organisational and technical advice on the course of action to protect the general and special categories of Personal Information
- ❖ Collect and review information about the processing of Personal Information
  - ✓ Customised PDF forms
  - ✓ Online submission of information
- ❖ Education
  - ✓ Customised in-house and web-based awareness and educational events for staff
  - ✓ Specialised training for Responsible Parties and Information Protection Officers
  - ✓ Specialised training for Business and IT management
- ❖ Provide point of contact for Data Subjects to submit information requests
  - ✓ Simple online form
  - ✓ Information Request Management System
  - ✓ Respond to Data Subject requests
- ❖ Conduct Audits of measures taken to satisfy Regulatory requirements
- ❖ Assist management remedy issues raised by the Regulator