HIPAA BASICS
- Security Rule

Presented to
HIPAA Summit III

October 26, 2001

Tom Hanks
Director Client Services
Health Care Practice
Tom.Hanks@us.pwcglobal.com
(312) 701-2466

PRICEWATERHOUSECOOPERS

Working Together: HIPAA Security and Privacy

- Security NPRM
- Privacy Rule – final 4/14/2001
- Final Security rule will be harmonized with the final Privacy rule
- Final Privacy rule prepares us for the final Security rule

Privacy and Security– Who Are Covered Entities

- Clearinghouses
- Health Plans
- Health Care Providers
  - ONLY those that transmit electronic transactions

Security *vs.* Privacy... Definitions

Security

- **Ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss**

Privacy

- **Defines who is authorized to access information (the right of individuals to keep information about themselves from being disclosed)**
- **Individual’s rights**

Working Together:
HIPAA Security and Privacy

- Scalability of requirements
- Access controls
- Internal use & disclosure
- What kind of “safeguards” are required

Security – Safeguarding PHI

- Establish and maintain *reasonable* and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and *availability* of the information
- Requirements are technology neutral - - each organization determines the technology to achieve outcome
- No proscribed implementation

Security – Safeguarding PHI (cont'd)

- Reasonably required to protect from intentional or unintentional violation
- Each health care business determines their own needs
- Implementation varies according to size and type of entity
- Must consider cost

Privacy – Safeguarding PHI

- Must have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI
- *Reasonably* safeguard health information

Privacy – Safeguarding PHI - Reasonably?

- Common sense, flexible and scalable
- Implementation varies with size and type of activities
- Must consider cost
  - **Strike a balance between protecting privacy and cost**

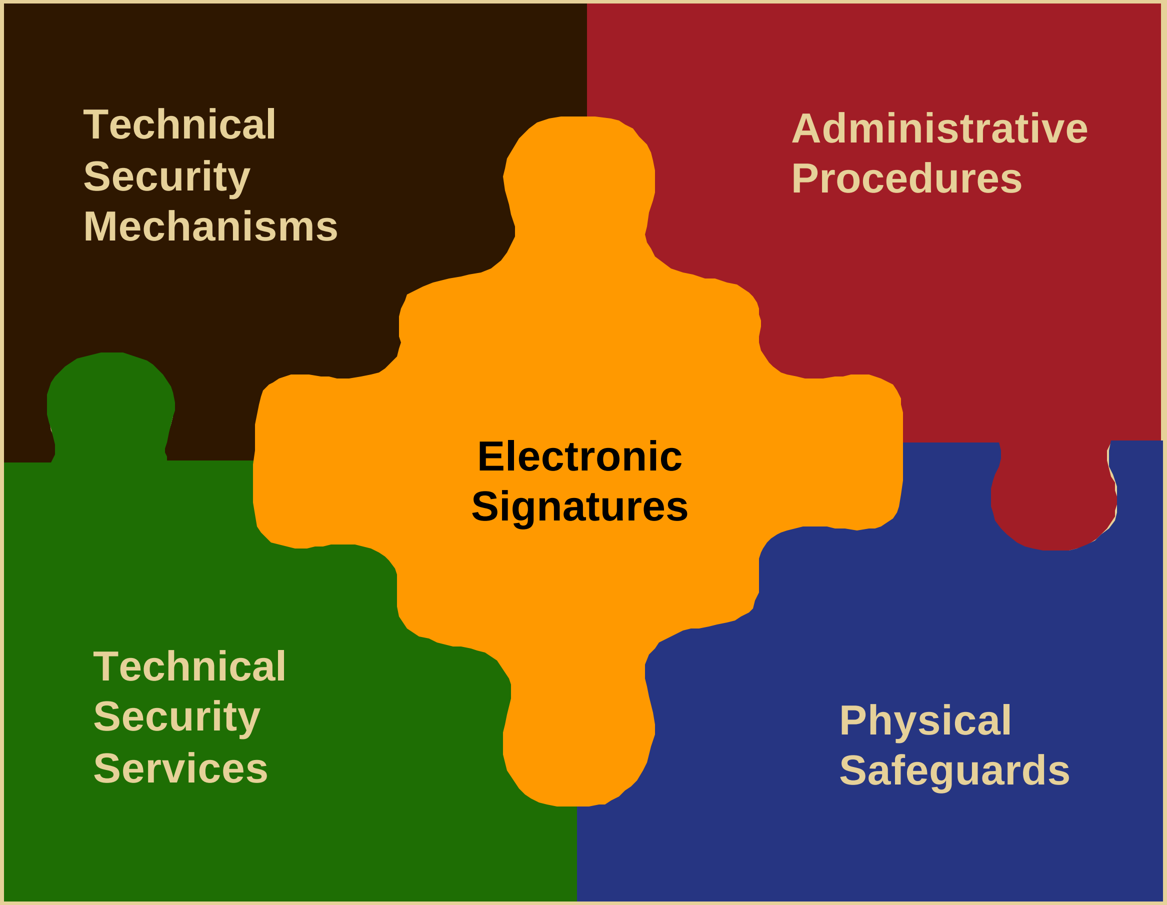
Privacy – Safeguarding of PHI

- Not required to guarantee the safety of PHI against all threats
- Theft of PHI may not be a violation if reasonable policies in place

Proposed HIPAA Security Regulations

Security Concepts:

- Comprehensive
- Technology-neutral
- Scalable


Technical Security Mechanisms
Administrative Procedures
Electronic Signatures
Technical Security Services
Physical Safeguards

Administrative Procedures

Certification

- Evaluation of computer and network security
- May be performed internally or externally

Chain of Trust Agreement

- Parties that exchange data electronically must contract to agree to protect transmitted data

<u>Definition:</u>

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures

Contingency Plan

- Requires periodic backups
- Requires emergency availability of critical facilities (criticality of data/systems must be determined)
- Requires disaster recovery procedures and testing

<u>Definition:</u>

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures (continued)

Formal Mechanism for Processing Records

- Documented policies and procedures for routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information

<u>Definition:</u>

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures (continued)

Information Access Control

- Formal, documented policies and procedures for granting different levels of access to health care information

Internal Audit

- Ongoing internal audit process
- In-house review of system activity records

Definition:

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures (continued)

Personnel Security

- Personnel must have appropriate clearances
- All personnel access to data must be authorized
- Maintenance personnel must be supervised

Definition:

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures (continued)

Security Configuration Management

- Documentation and inventory of hardware/software
- Installation/maintenance review and testing
- Virus checking software

<u>Definition:</u>

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures (continued)

Security Incident Procedures

- Instructions for reporting security breaches

Security Management Process

- Risk analysis/management
- A formal security policy with sanctions

__Definition:__

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures (continued)

Termination Procedures

- Documentation to end a user’s access
- Includes changing locks, return of keys/cards
- Removal of system access/user account

<u>Definition:</u>

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Administrative Procedures (continued)

Training

- Security must be part of day-to-day activities
- All personnel must receive awareness training

<u>Definition:</u>

Documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Physical Safeguards

Assigned Security Responsibility

- Must be assigned to individual or organization

Definition:

Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Physical Safeguards (continued)

Media Controls

- Policies and procedures governing receipt and removal of hardware/software into/out of a facility
- Includes access, accountability, backup, storage, and disposal

<u>Definition:</u>

Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Physical Safeguards

Physical Access Controls

- Policies and procedures to limit physical access
- Includes emergency mode operation, facility security and authorizations, maintenance records, need-to-know control and visitor logs

<u>Definition:</u>

Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Physical Safeguards (continued)

- Policy/Guideline on Workstation Use
  - Instructions for logging off, unattended terminals
- Secure Workstation Location
  - Safeguards to minimize unauthorized access
- Security Awareness Training
  - Required for all employees, agents, and contractors

Definition:

Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Technical Security Services (continued)

Access Control

- Restrict/allow access only to privileged users
- Must have procedure for emergency access
- Context, role, or user based access control
- Encryption is optional

<u>Definition:</u>

Processes that are put in place to protect information and to control individual access to information.

Privacy – Access Controls

- **Privacy rule establishes access**
- **Role based**
- **Identify persons or class of persons that need access to PHI**
- **Limit access to only the PHI needed to perform their job**

Privacy – Access Controls Reasonable Efforts

- Takes into account the ability of the entity to configure its record system to allow selective access
- Practicality of organizing systems to allow this capacity
- Recognizes limitations on parsing paper records

Technical Security Services (continued)

Audit Controls

– Mechanisms to record and examine system activity

Authorization Control

– Mechanism for obtaining consent for the use and disclosure of health information

__Definition:__

Processes that are put in place to protect information and to control individual access to information.

Security – Audit Trails

- Audit trails required – no implementation provision
- The data collected and potentially use to facilitate a security audit
- Internal audit requirement to review records of system activity – audit trail

Privacy – Defines Audit Trail Expectations

- **Audit trails do not usually record each time a record is used or reviewed**
- **Audit trails typically record each time a sensitive record is altered**
- **Important to coordinate Accounting for Disclosure with Audit Trails in Security**

Privacy
– Accounting for Disclosure

Accounting Not an Audit Trail

- Name and address, if known, of person or entity receiving the PHI
- Date of each disclosure
- Brief description of information disclosed
- Purpose for disclosure or copy of individual’s authorization

Technical Security Services (continued)

Authorization Control

- Mechanism for obtaining consent for the use and disclosure of health information

Definition:

Processes that are put in place to protect information and to control individual access to information.

Technical Security Services (continued)

Automatic logoff

Data Authentication

- Proof that data has not been altered or destroyed in an unauthorized manner
- Suggest checksum, double keying, digital signature

__Definition:__

Processes that are put in place to protect information and to control individual access to information.

Technical Security Services (continued)

Entity Authentication

- Proof that user is who he/she claims to be
- Requires unique userID
- Password is the baseline
- Optional biometrics, PINs, physical tokens, etc.

Definition:

Processes that are put in place to protect information and to control individual access to information.

Technical Security Mechanisms

Required If Using Open Networks

- Access Controls
- Alarm
- Audit trail
- Encryption
- Entity authentication
- Event reporting
- Integrity controls
- Message authentication

Definition:

Processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.

Electronic Signatures

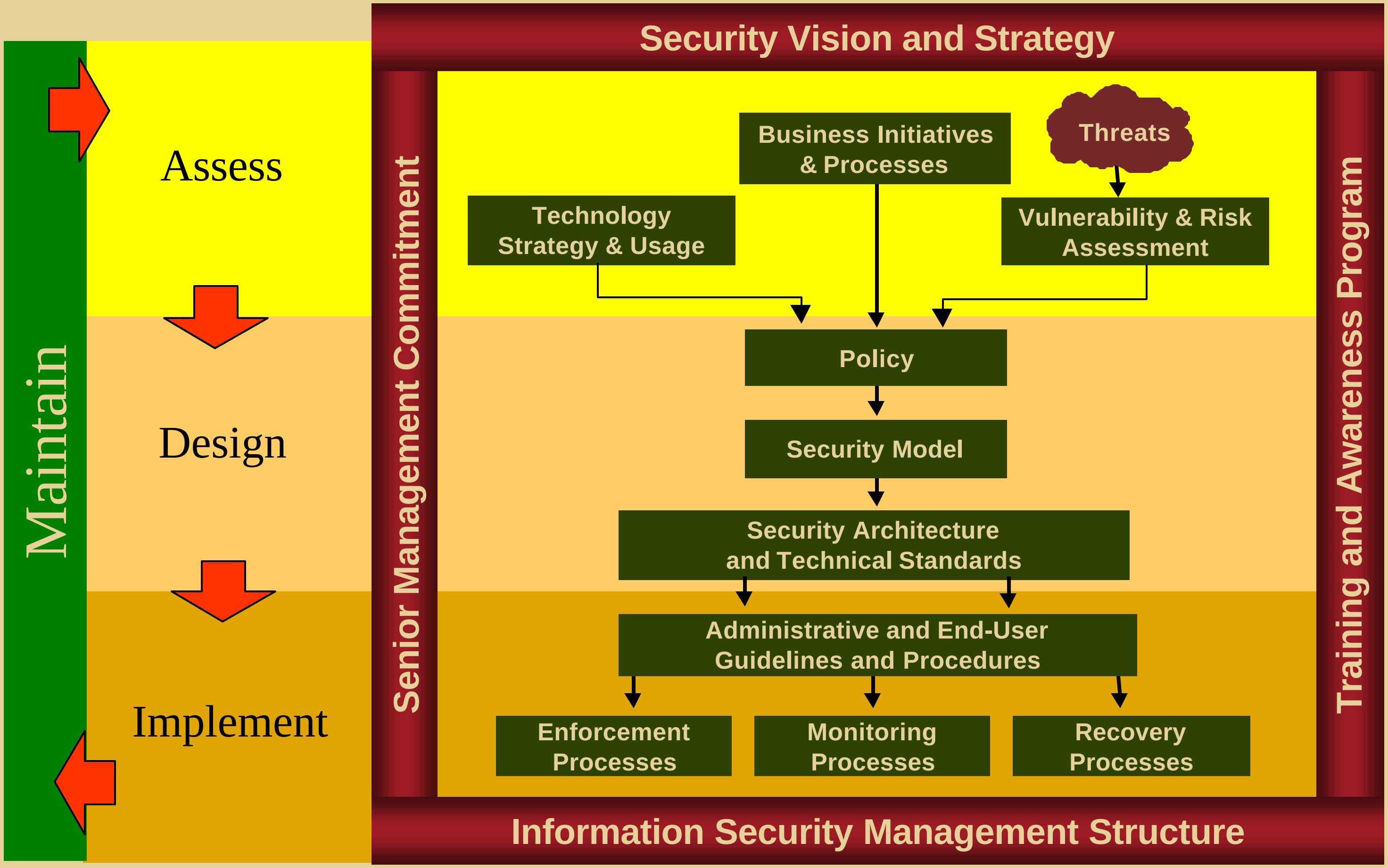
Electronic Signatures

- Being removed from Security Rule
- Will not conflict with E-Sign Law

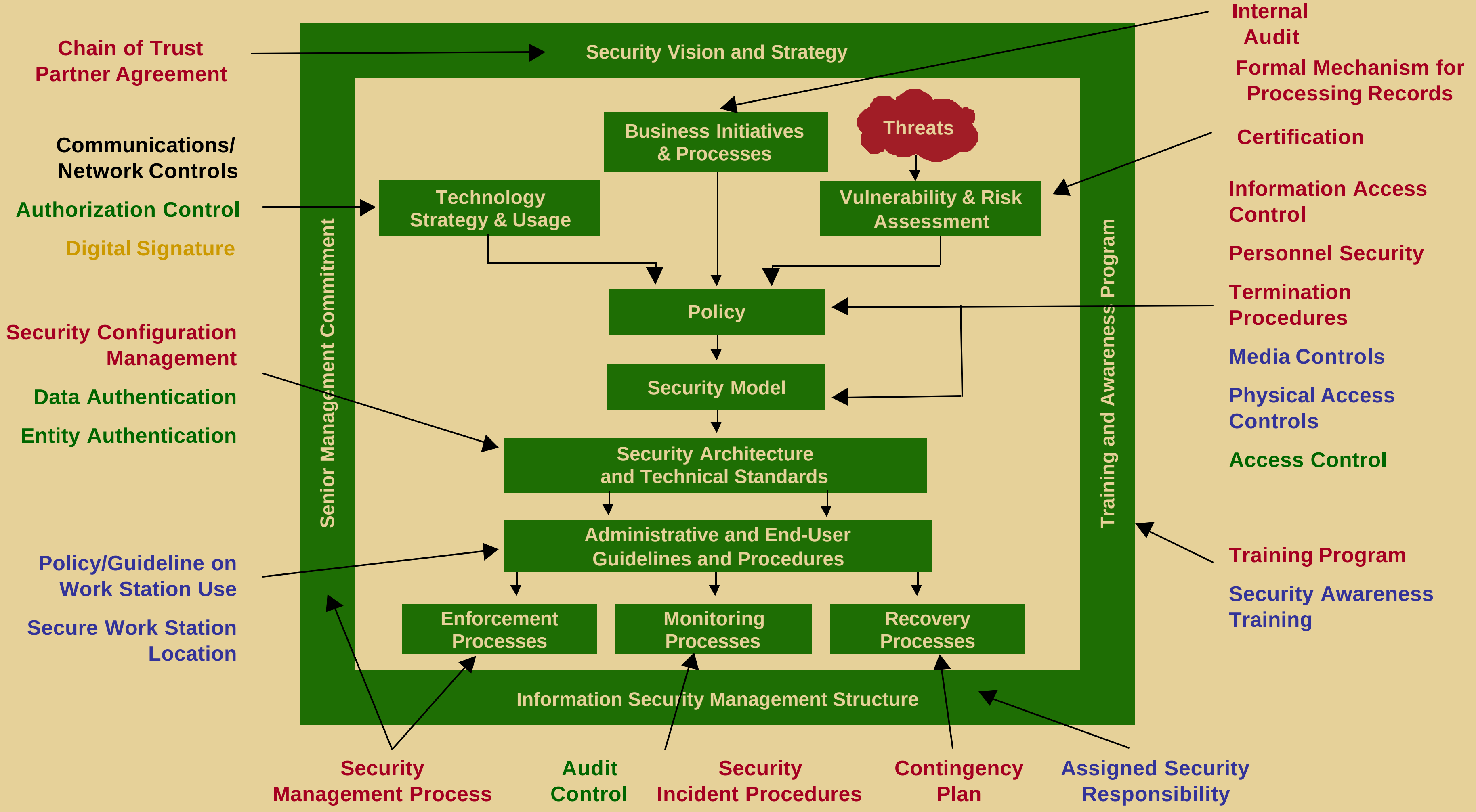
<u>Definition:</u>

An electronic signature refers to the act of attaching a signature by electronic means. The electronic signature process involves authentication of the signer's identity, binding of the signature to the document and non-alterability after the signature has been affixed to the document. The generation of electronic signatures requires the successful identification and authentication of the signer at the time of the signature.

Enterprise Security
-Good Practice Model


Maintain
Assess
Design
Implement
Security Vision and Strategy
Senior Management Commitment
Training and Awareness Program
Information Security Management Structure
Business Initiatives & Processes
Threats
Technology Strategy & Usage
Vulnerability & Risk Assessment
Policy
Security Model
Security Architecture and Technical Standards
Administrative and End-User Guidelines and Procedures
Enforcement Processes
Monitoring Processes
Recovery Processes

HIPAA Security Requirements - Mapped to Good Practice Model



Security Vision and Strategy

Senior Management Commitment

Training and Awareness Program

Business Initiatives & Processes

Threats

Technology Strategy & Usage

Vulnerability & Risk Assessment

Policy

Security Model

Security Architecture and Technical Standards

Administrative and End-User Guidelines and Procedures

Enforcement Processes

Monitoring Processes

Recovery Processes

Information Security Management Structure

Chain of Trust Partner Agreement

Communications/ Network Controls

Authorization Control

Digital Signature

Security Configuration Management

Data Authentication

Entity Authentication

Policy/Guideline on Work Station Use

Secure Work Station Location

Internal Audit

Formal Mechanism for Processing Records

Certification

Information Access Control

Personnel Security

Termination Procedures

Media Controls

Physical Access Controls

Access Control

Training Program

Security Awareness Training

Security Management Process

Audit Control

Security Incident Procedures

Contingency Plan

Assigned Security Responsibility

Wrap-Up

- Security requirements are basic – each entity defines their own needs based on assessment and..
  - Type & size of business
  - Taking cost into consideration
- Both Security and Privacy rules address safeguarding health information
- Final Security Rule will not conflict with final privacy rule

Resources

- PwC Health Care
- **www.pwcglobal.com/healthcare**
- WEDI web site
  - www.wedi.org
- AFEHCT web site
  - www.afehct.org
- EHNAC web site
  - www.ehnac.org

Resources

- DHHS - administrative simplification
  - aspe.dhhs.gov/admnsimp/index.htm
- DHHS data council web site
  - aspe.dhhs.gov/datacncl/
- NCVHS Web Site
  - ncvhs.hhs.gov

Questions and Discussion

Tom Hanks

Director Client Services

(312) 701-2466

Tom.Hanks@us.pwcglobal.com

p w c