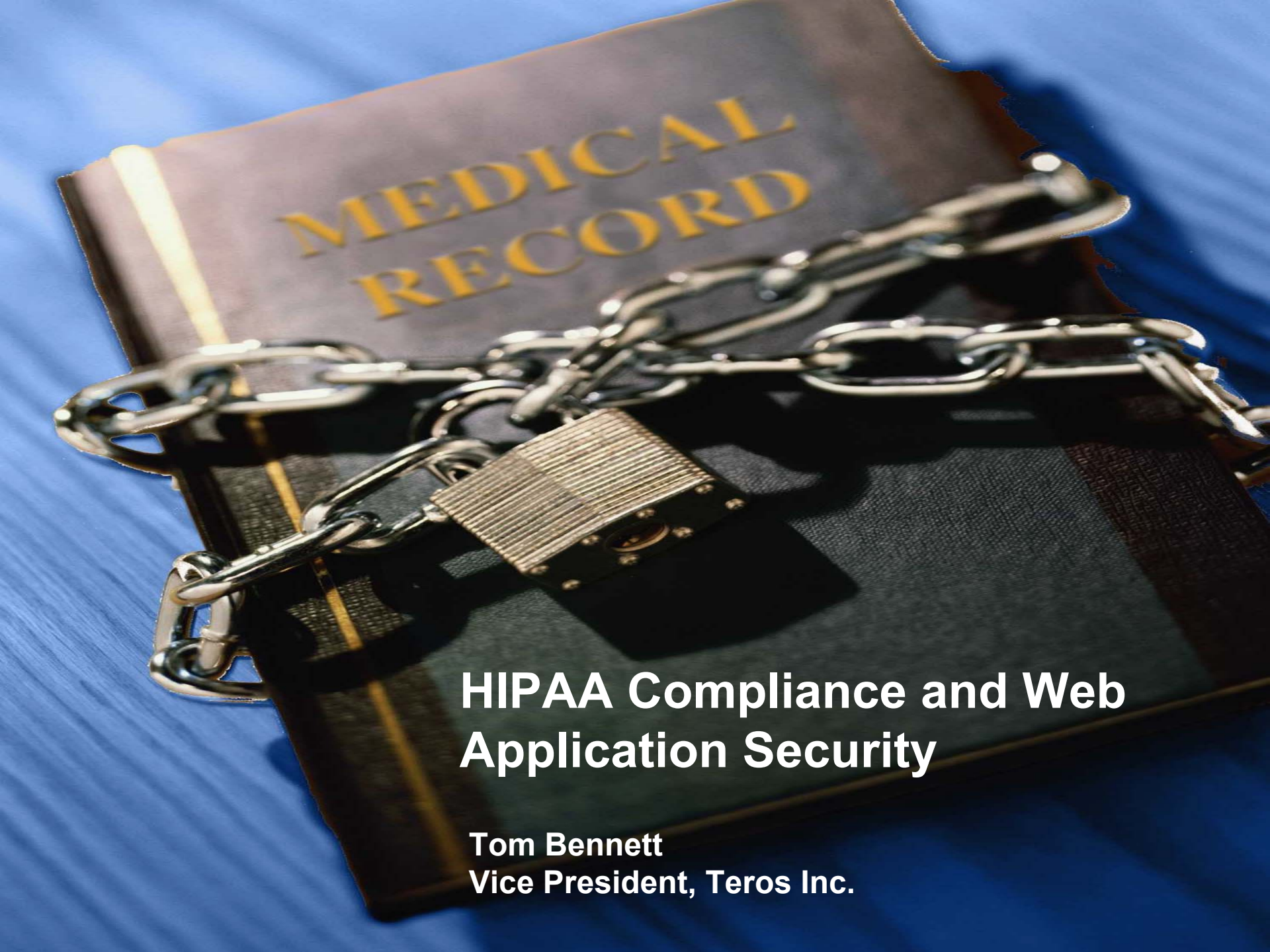


HIPAA Compliance and Web Application Security

Tom Bennett
Vice President, Teros Inc.

TEROS™
Protect With Precision.

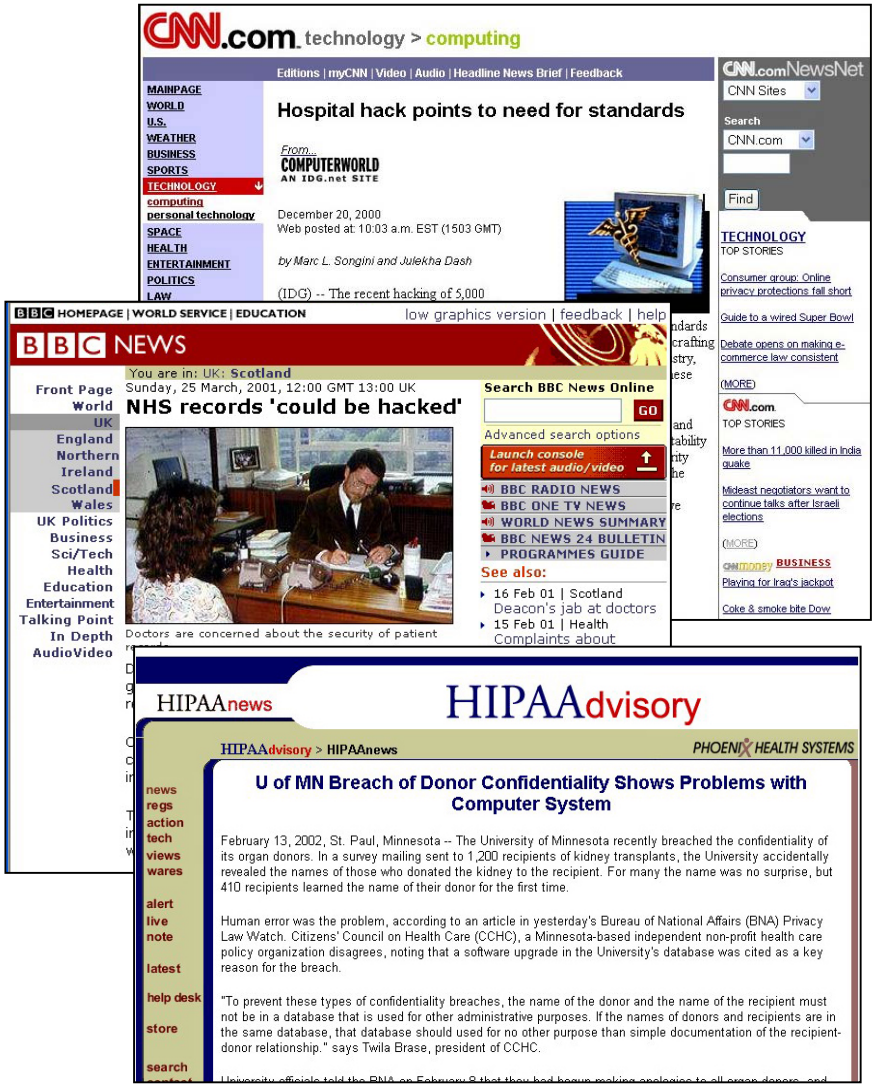
Agenda

- **HIPAA Overview**
  - Current Status
- **Basics**
  - Electronic Data Exchange
  - Web Applications
- **Typical Healthcare Web Applications**
- **Vulnerabilities Overview**
- **Identity Theft and Database Breach**
  - Compliance and Liability Implications
- **What you can do about it!**

TEROS™
Protect With Precision.

Web Applications are a Hacker's the Entry Point

- **Online Health Services are Vulnerable**
  - 70% of attacks are at web applications
  - SSN, Private Data and Account #s most vulnerable to theft and compromise.
- **Existing security does not stop web applications attacks**
  - Firewalls, IDS and SSL protect networks, not individual applications
- **Security breaches cost millions**
  - Lost revenue, Brand Erosion, Customer Retention, PR
- **Web Application Security is Required!**
  - HIPAA means you are responsible
  - Database Breach Act—Liability!



TEROS™
Protect With Precision.

What are the consequences?

- **Defacement is the least of your worries!**
  - Identity Theft
  - Lost revenue
  - System repair and downtime
- **Identity Theft is HUGE**
  - Short term PR, lost customers longer term
  - Now you are liable!
- **You may be an unwilling facilitator in someone else's disaster**
  - Cross-site attacks
  - Application as entry point to corporate networks!

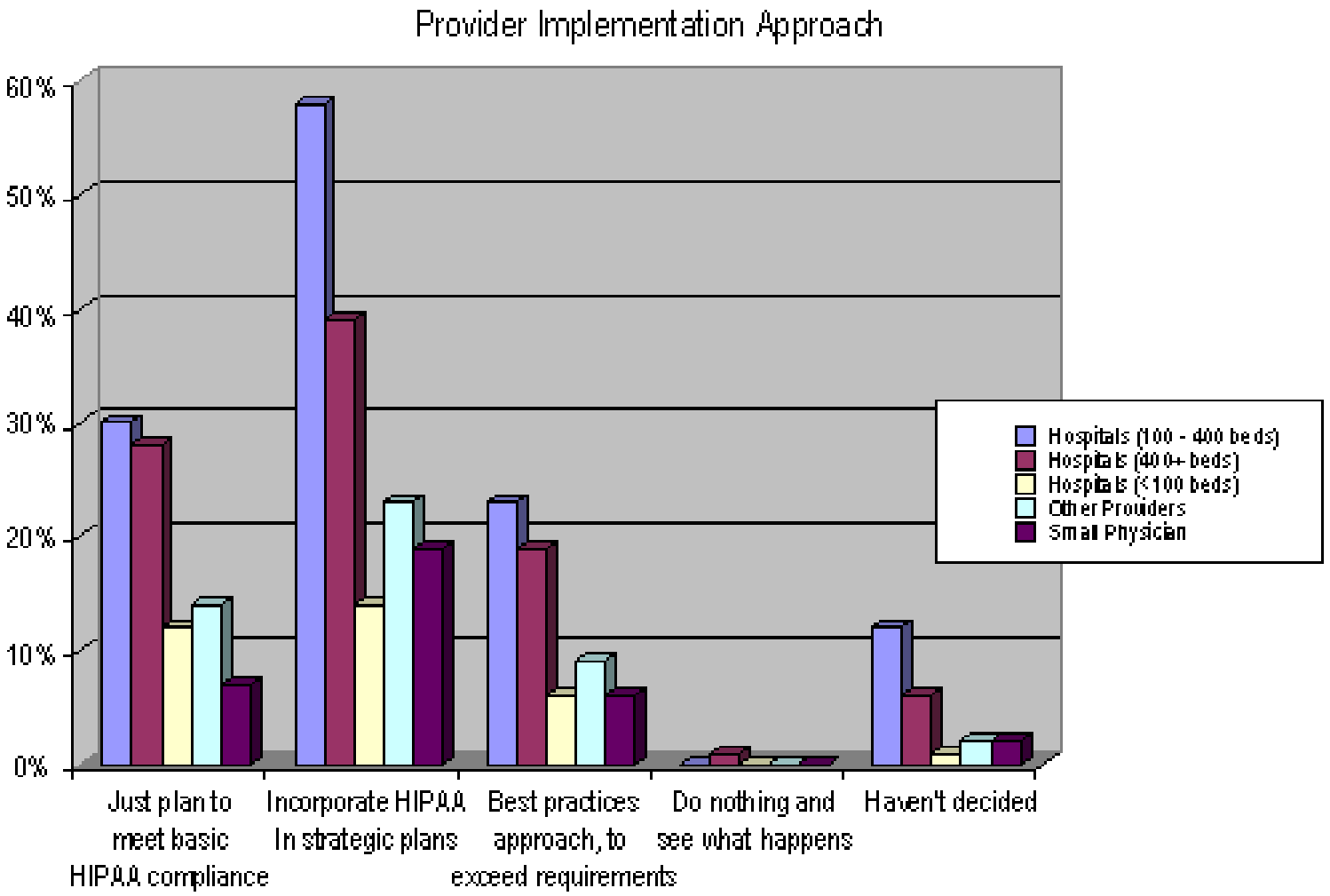
TEROS™
Protect With Precision.

Healthcare Insurance Portability and Accountability Act

- **Comprehensive security programs**
- **Administrative Simplification**
- **Who is Affected?**
  - Covered Entities
    - Health Plan
    - Health Care Clearinghouse
    - Health Care Provider
  - Business Associates
- **Penalties for Non-compliance**
  - Civil
  - Criminal

TEROS™
Protect With Precision.

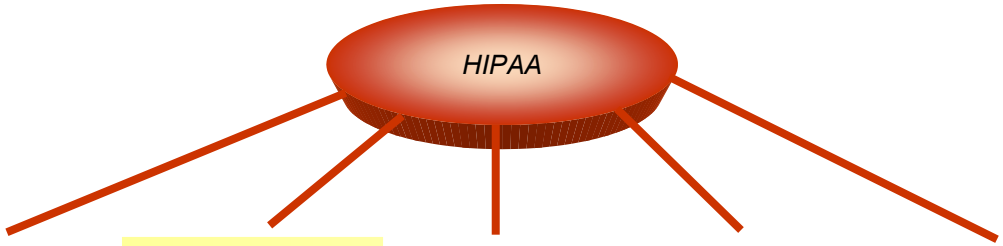
What are people doing?



Winter 2002 Survey - www.hipaadvisory.com

TEROS™
Protect With Precision.

HIPAA - Title II



Title I

- Health insurance access, portability and renewal

Title II

- Fraud and Abuse
- Medical Liability Reform
- Administrative Simplification
  - Electronic Transaction Standards (EDI)
    - For 9 key payor transactions
    - Includes clinical code sets
    - Includes key identifiers
  - Security Standards
    - For protecting electronic health information
  - Privacy Standards
    - To spell out permissible uses of patient identifiable healthcare information

Title III

- Medical Savings Accounts
- Tax deduction provisions

Title IV

- Group health plan provisions

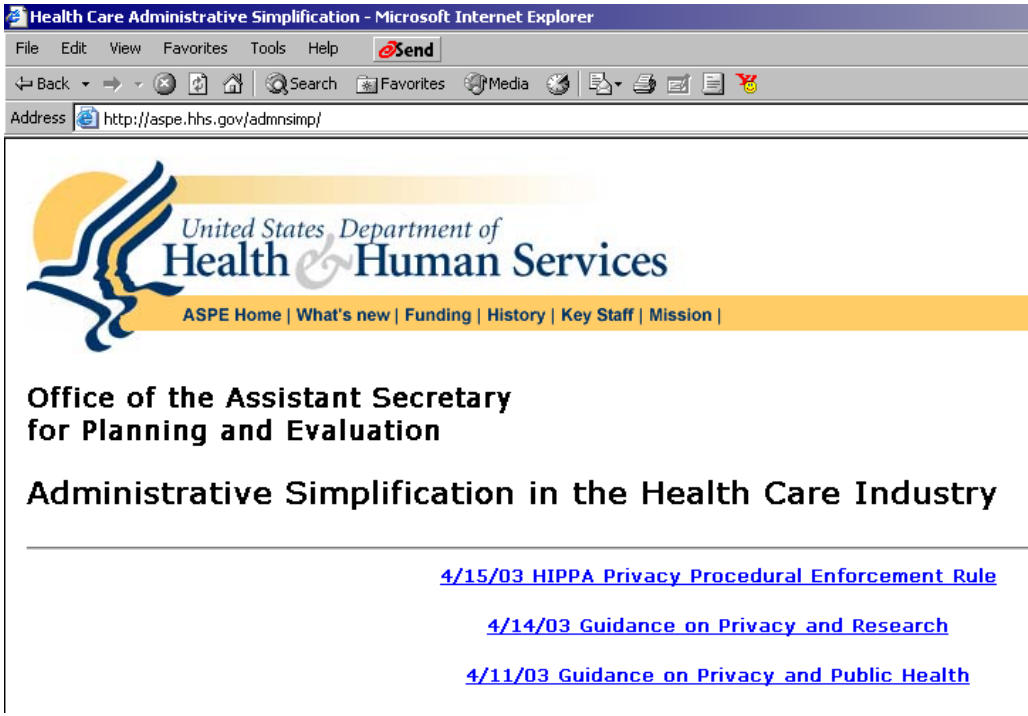
Title V

- Revenue offset provisions

TEROS™
Protect With Precision.

Administrative Simplification Regulatory Requirements

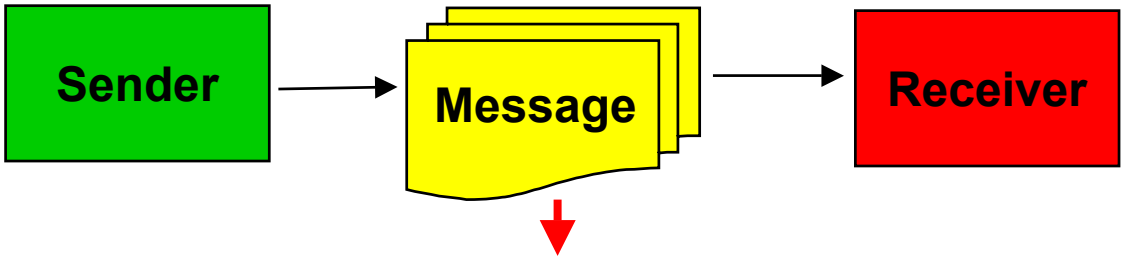
- **Electronic Data Interchange Transaction Sets Standardized Codes Sets Standardized Identifiers (EDI/TCI)**
  - Trading Partner
  - Transaction
  - Standard Setting Organization (SSO)
  - Transaction Sets
  - Code Sets
  - Unique Identifiers



TEROS™
Protect With Precision.

Trading Partner

In Electronic Data Interchange (EDI) this generally applies to two parties engaged in the exchange of business data through electronic means.



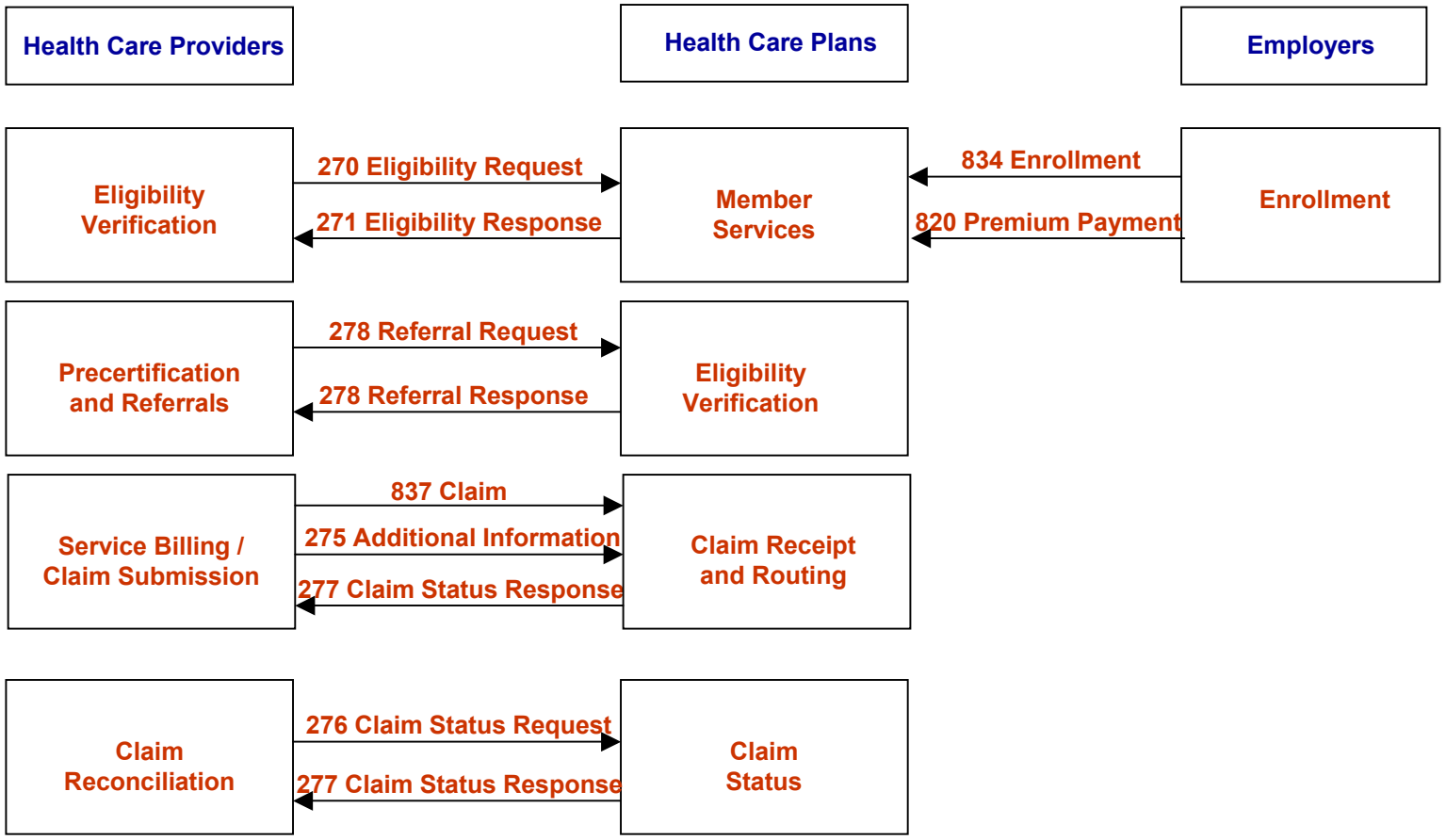
SEGMENT: ST - Transaction Set Header
LEVEL: Header
LOOP: None
MAX USAGE: 1
PURPOSE: To indicate the start of a transaction set and assign a control number to it.
COMMENTS: This segment also identifies the transactin set ID ("830" = Planning Schedule with release Capability). The control number (ST02) in the header must match the control number in the transactin set trailer (SE02).
EXAMPLE: ST*830*000001~

Element					
Example Value	ID	Number	Length Min/Max	Name	Comments
ST				Segment ID	Transaction set Header
830	ST01	143	3/3	Transaction Set ID	Always = "830"
000001	ST02	329	6/6	Transaction Set Control Number	Unique number assigned to each transaction set within a functional group starting at 000001 and incrementing by +1 for each subsequent transaction set.

- *Health Care claims or equivalent encounter information.*
- *Health Care payment and remittance advice.*
- *Coordination of benefits.*
- *Health Care claim status.*
- *Enrollment and disenrollment in a health plan.*
- *Eligibility for a health plan.*
- *Health plan premium payments.*
- *Referral certification and authorization.*
- *First report of injury.*
- *Health claims attachments.*
- *Other transactions that the Secretary may prescribe by regulation.*

TEROS™
Protect With Precision.

X.12 Transaction Sets

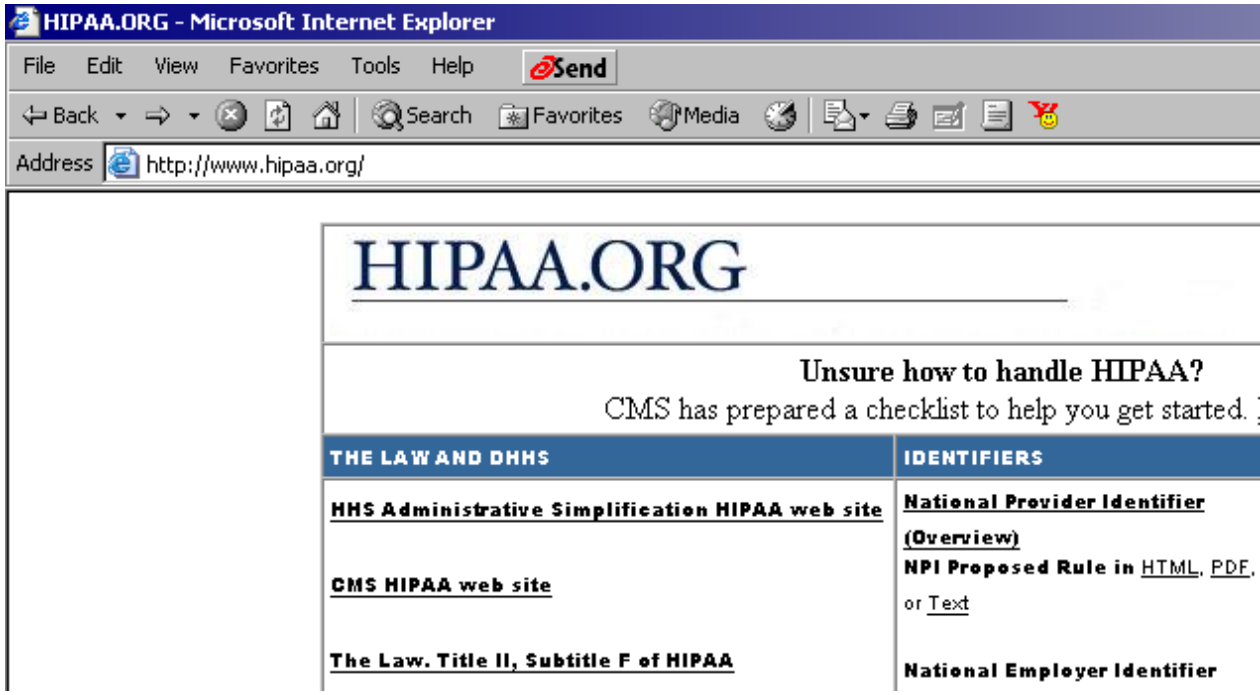


ASCX12
The Accredited Standards Committee (ASC) X12

TEROS™
Protect With Precision.

Privacy and Security

- **Privacy Ruling -** *Who Can Disclose Data*
  - The need for information security to ensure privacy is delineated: .It is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure..
- **Security Ruling -** *Protecting Data*
  - Mandates safeguards for physical storage and maintenance, transmission and access to individual information.



TEROS™
Protect With Precision.

Protected Health Information (PHI)

"PHI" means any information allowing direct or indirect identification of an individual through one or more specific characteristics of the individuals' physical, physiological, or mental condition. Such information includes, but is not limited to:

- Name
- Address
- E-Mail Address
- Social Security Number
- Password (if used to access the site)
- Bank Account Information
- Credit Card Information

Any combination of Data that could be used to identify a consumer, such as the consumer's birth date, zip code and gender.

TEROS™
Protect With Precision.

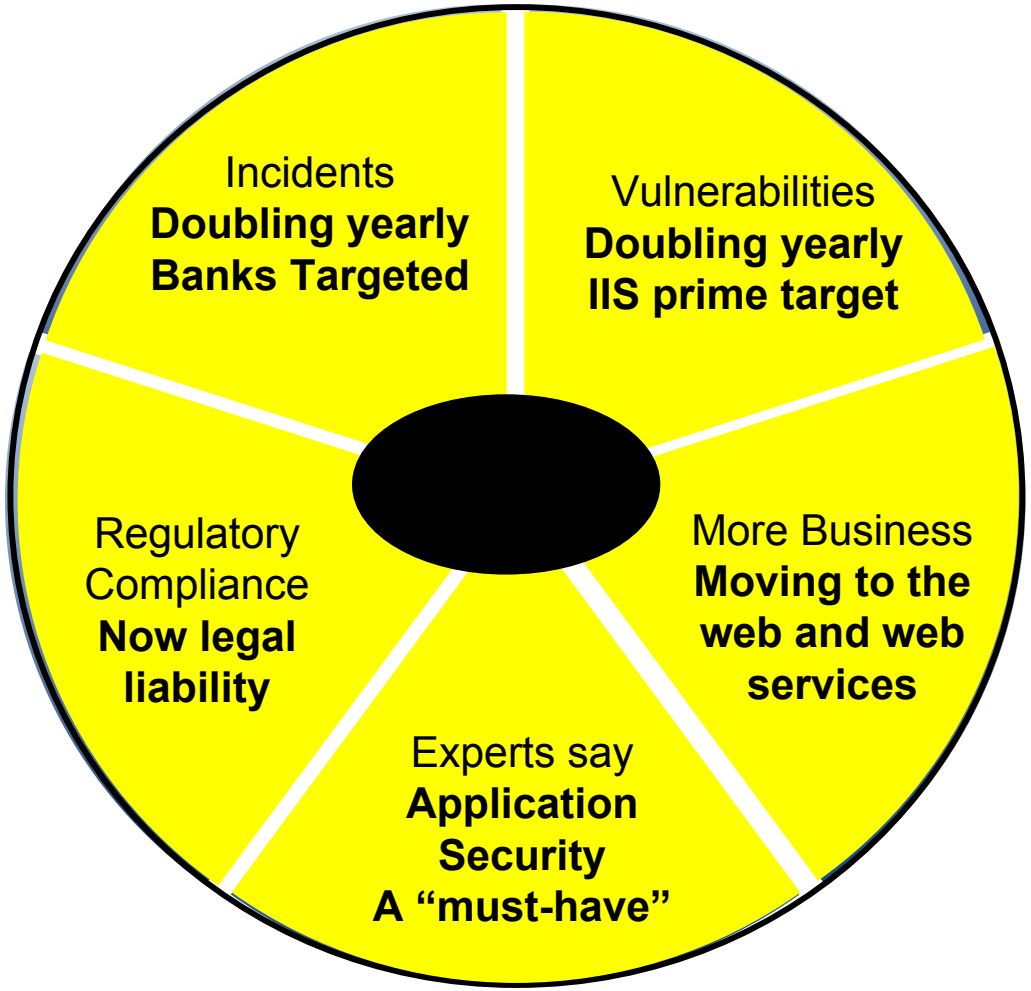
Security & Privacy

- **Privacy - an individual's rights to control access and disclosure of their protected or individually identifiable healthcare information (IIHI)**
  - Establish authorization requirements
  - Establish administration requirements
  - Establish individual rights
  - Establish regulations for use or disclosure of Protected Health Information ("PHI")
- **Security - an organization's responsibility to control the means by which such information remains confidential**
  - Physical Safeguards
  - Administrative Procedures
  - **Technical Security Services**
  - **Technical Security Mechanisms**

Web Application Security

TEROS™
Protect With Precision.

Web Applications need protection

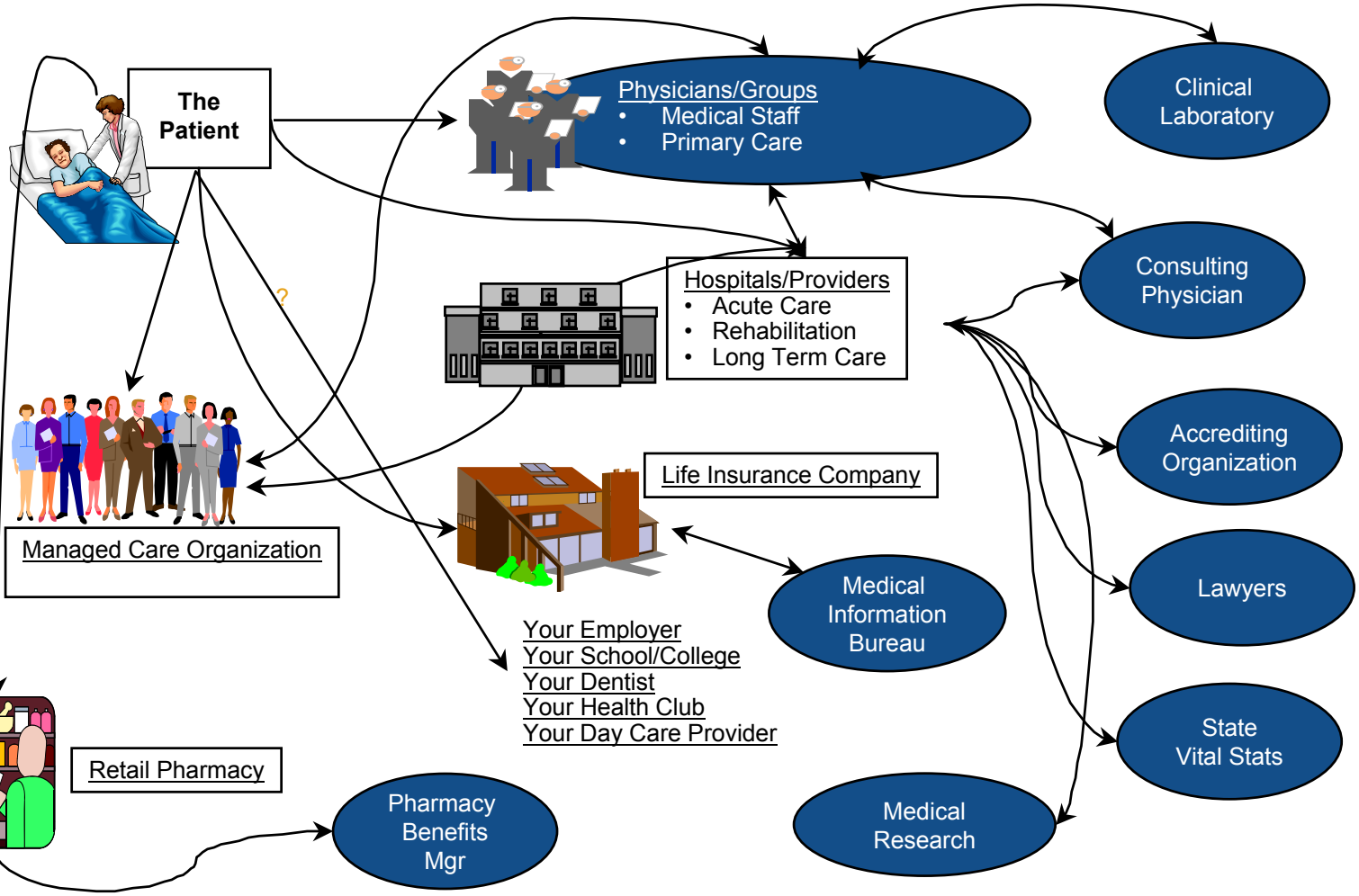


"Enterprises must ensure that
"The number of
"The primary impediment to web services deployment is lack of security..."
(Everyone)
Gartner August 2003
Benjamin Wright

Web Vulnerability and Incident Explosion

TEROS™
Protect With Precision.

HIPAA Information Flow



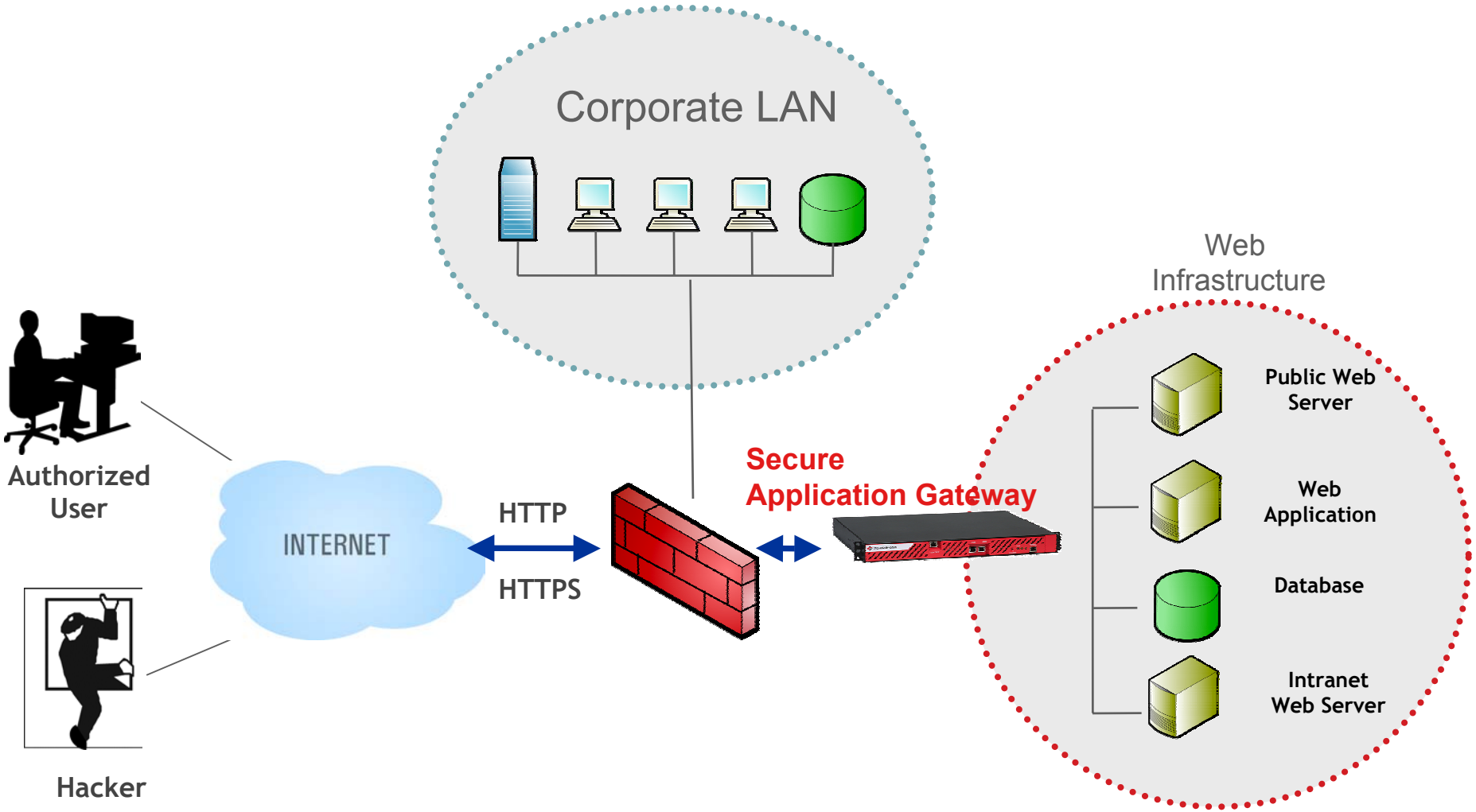
TEROS™
Protect With Precision.

Typical Healthcare Web Applications

- **Patient**
  - Appointment Scheduling Confirmation
  - Benefits Reviews
  - Prescription Fulfillment
- **Physicians Groups, Hospitals, Pharmacies etc.**
  - Patient Records
    - *Patient/Care Summaries*
    - *Prescriptions Assignment*
    - *Appointment Scheduling*
- **Health/Life Insurance Companies**
  - Benefits Plans
    - *Summaries of Benefits*
    - *Designation of Beneficiaries*
- **Managed Care Organizations**
  - Patient Records
    - *Patient/Care Summaries*
    - *Summaries of Benefits*
- **Lawyers, Accrediting Organizations, Medical Information/Research**
  - Healthcare Provider Records
  - Benefits Plans

TEROS™
Protect With Precision.

You need to protect your web infrastructure…



Web Security Gateways do what firewalls, IDS, and VPN's do for the network

TEROS™
Protect With Precision.

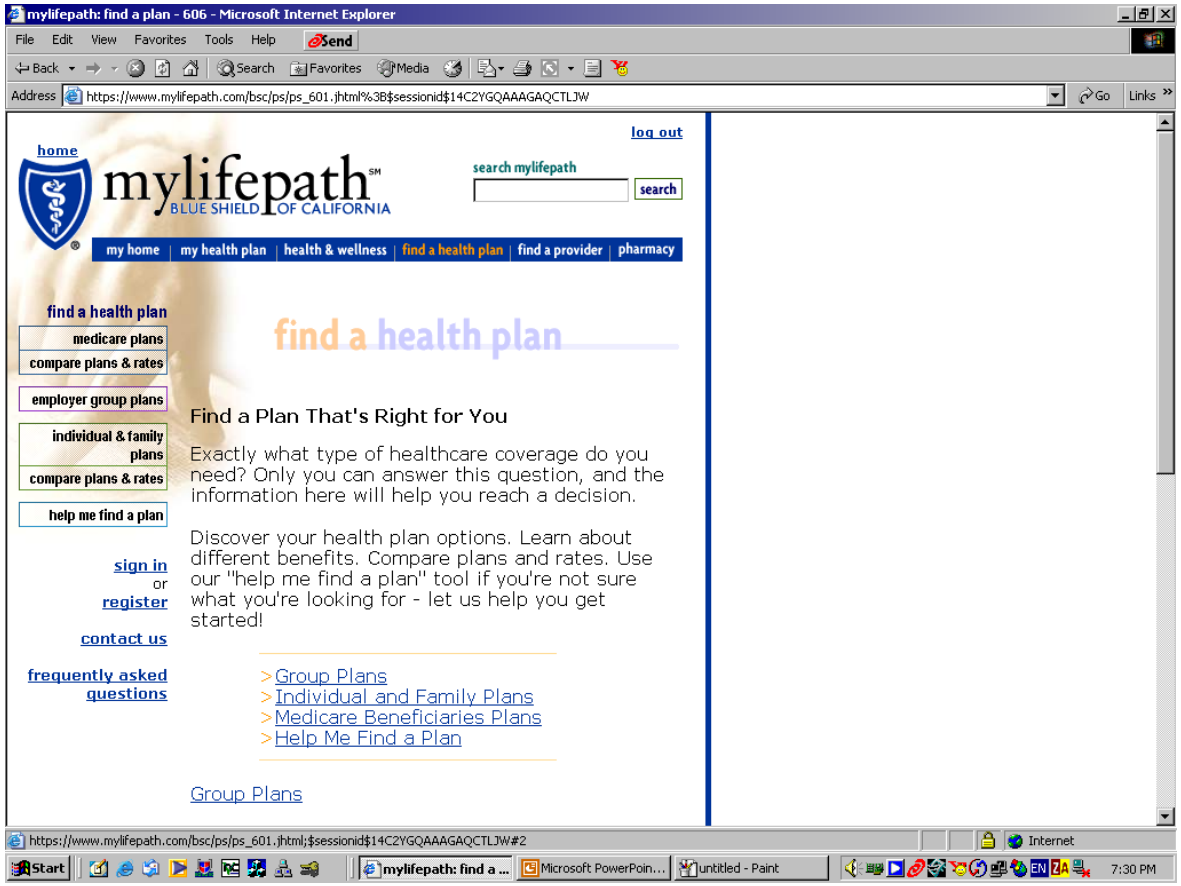
Complete Web Application Security

- **Protects 16 of 16 application vulnerability classes**
- **Protects 10 of 10 OWASP Top Ten**
- **ALL IIS web vulnerabilities: Automatically Protected**
- **ALL web worms - Code Red, Nimda, …: Automatically Protected**
- **ALL published exploits in Hotmail: Automatically Protected**

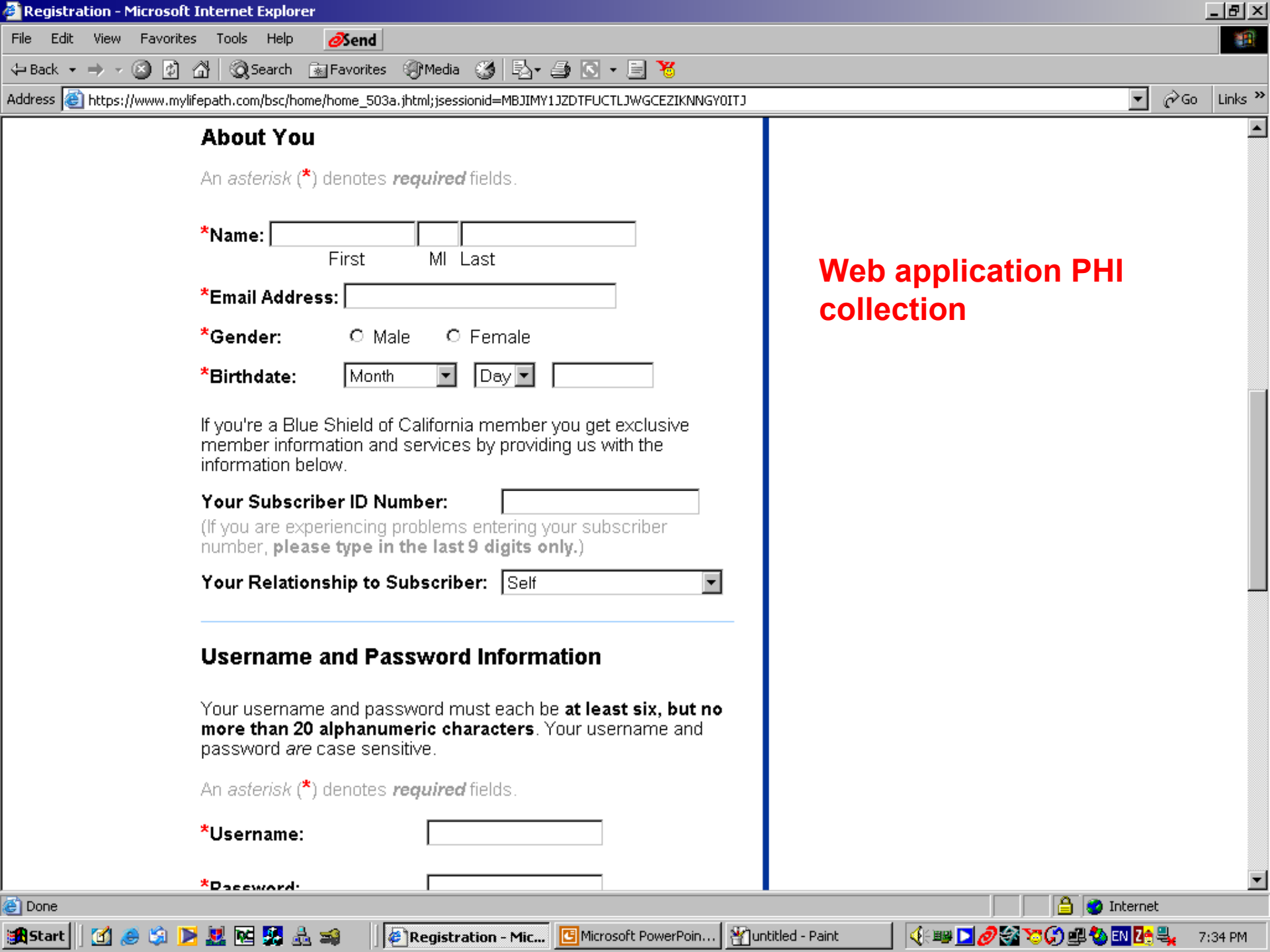
Vulnerability Score Card		
1	Buffer Overflow Exploits	☑
2	CGI-BIN Param Manipulation	☑
3	Form/Hidden Field Manipulation	☑
4	Forceful Browsing	☑
5	Cookies/Session Poisoning	☑
6	Broken ACLs / Weak Passwords	☑
7	Cross-site Scripting (XSS)	☑
8	Command Injection	☑
9	SQL Injection	☑
10	Error Triggering Sensitive Information Leaks	☑
11	Insecure use of Crypto	☑
12	Server Misconfiguration	☑
13	Backdoors & Debug Options	☑
14	Web-site Defacement	☑
15	Well-known Platform Vulnerabilities	☑
16	Unpublished Attacks	☑

TEROS™
Protect With Precision.

Typical Vulnerabilities



Threats Examples.exe


Registration - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites Media
Address https://www.mylifepath.com/bsc/home/home_503a.jhtml;jsessionid=MBJIMY1JZDTFUCTLJWGCEZIKNNGYOITJ
Go Links
About You
An asterisk (*) denotes required fields.
*Name:
First MI Last
*Email Address:
*Gender: Male Female
*Birthdate: Month Day
If you're a Blue Shield of California member you get exclusive member information and services by providing us with the information below.
Your Subscriber ID Number:
(If you are experiencing problems entering your subscriber number, please type in the last 9 digits only.)
Your Relationship to Subscriber: Self
Username and Password Information
Your username and password must each be at least six, but no more than 20 alphanumeric characters. Your username and password are case sensitive.
An asterisk (*) denotes required fields.
*Username:
*Password:
Web application PHI collection
Done
Internet
Start
Registration - Mic...
Microsoft PowerPoin...
untitled - Paint
7:34 PM


mylifepath: find a plan - 606 - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites Media
Address https://www.mylifepath.com/bsc/ps/ps_601.jhtml%3B$sessionid$14C2YGQAAAGAQCTLJW
Go Links
log out
home
mylifepath℠
BLUE SHIELD OF CALIFORNIA
search mylifepath
search
my home | my health plan | health & wellness | find a health plan | find a provider | pharmacy
find a health plan
medicare plans
compare plans & rates
employer group plans
individual & family plans
compare plans & rates
help me find a plan
sign in
or
register
contact us
frequently asked questions
find a health plan
Find a Plan That's Right for You
Exactly what type of healthcare coverage do you need? Only you can answer this question, and the information here will help you reach a decision.
Discover your health plan options. Learn about different benefits. Compare plans and rates. Use our "help me find a plan" tool if you're not sure what you're looking for - let us help you get started!
>Group Plans
>Individual and Family Plans
>Medicare Beneficiaries Plans
>Help Me Find a Plan
Group Plans
Blue Cross/Shield of California Web application
SSL Session
https://www.mylifepath.com/bsc/ps/ps_601.jhtml;$sessionid$14C2YGQAAAGAQCTLJW#2
Internet
Start
mylifepath: find a ...
Microsoft PowerPoin...
untitled - Paint
7:30 PM

home_503a[1] - Notepad

File Edit Format Help Send

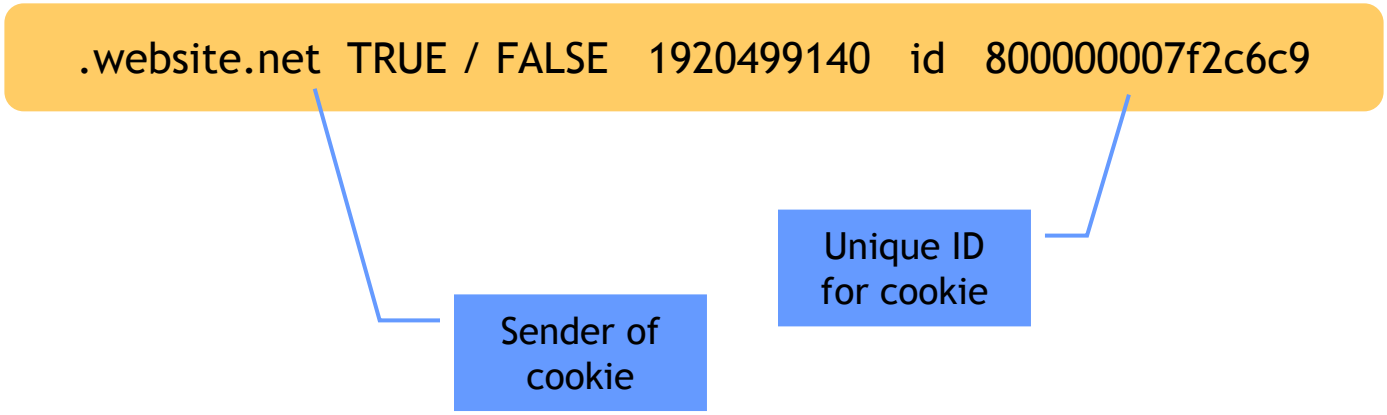
```
        </TD>
/TR>

TR>
        <TD><IMG height=10 src="/bsc/images/clearPixel.gif" width=1 border=0></TD>
/TR>

TR>
        <TD colspan="5" valign="top">

                <TABLE width="300" cellspacing="0" cellpadding="0" border="0">
                        <TR>
        <TD valign="middle" class="hw-normal" nowrap><b><font color="red"><big>*</big></font>Email Address:</b> </TD>
        <TD align="left"><input name="email"  size="33" maxlength="50" value=""
        ><input type="hidden" name="_D:email" value=" ">
        </TD>
                        </TR>
                        <TR>
                                <TD><IMG height=10 src="/bsc/images/clearPixel.gif" width=1 border=0></TD>
                        </TR>
                        <TR>
        <TD valign="middle" class="hw-normal"><b><font color="red"><big>*</big></font>Gender:</b></TD>
        <TD align="left" class="hw-normal">
                <input type="radio" value="M"


andler.value.sex" value=" "> Male     
                <input type="radio" value="F"
                name="/bsc/ui/BSCProfileHandler.value.sex"><in                                    ue.sex"
        </TD>
        </TR>
                        <TR>
                                <TD><IMG height=10 src="/bsc/images/clearPixel.gif" width=1 border=0></TD>
                        </TR>
        <TR>
        <TD valign="middle" class="hw-normal"><b><font color=red><big>*</big></font>Birthdate:</b>  </TD>
        <TD align="left" class="hw-normal" nowrap>
ize="1"
nth" name="/bsc/ui/BSCProfileHandler.dobMonth">
alue="0">Month</option>
alue="1">January</option>
alue="2">February</option>
alue="3">March</option>
alue="4">April</option>
alue="5">May</option>
alue="6">June</option>
alue="7">July</option>
alue="8">August</option>
alue="9">September</option>
alue="10">October</option>
alue="11">November</option>
alue="12">December</option>
```

Literal paths in web app coding

Start | Registration ... | Microsoft Po... | untitled - Paint | home_503a... | 7:36 PM

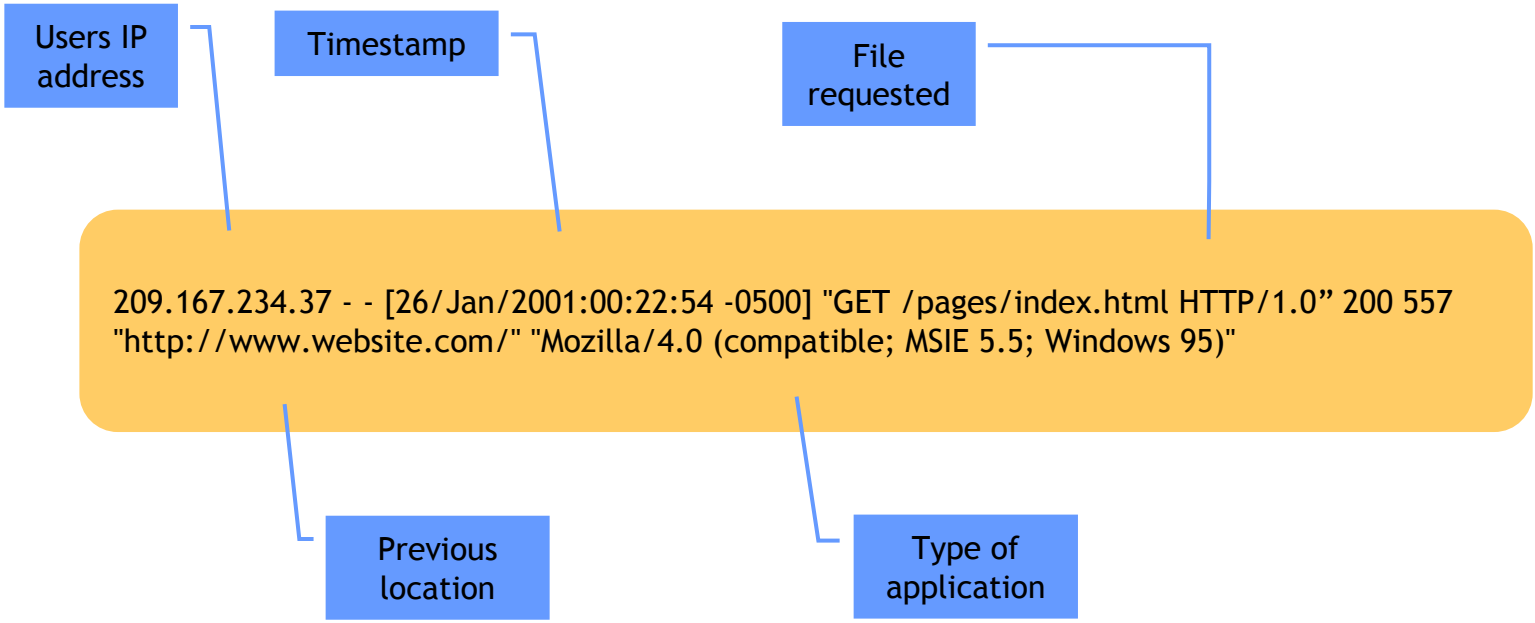
Cookies

Cookies can link identity and activity across distinct organizations



Web Servers

Web servers see more than the user knows…



TEROS™
Protect With Precision.

Recommendations

Full disclosure about …

- Clients' use of self cookies
- Use of third party cookies on clients web site
- Use of third party 1x1 clear pixel tags on clients web site
- Third party/partners' involvement in data collection and analysis

Prominently display link to privacy statement on all web pages:

- Place "Privacy" link at top of page (versus bottom, where most companies place it) and make it very prominent (I.e., larger font, bolded, etc.)

TEROS™
Protect With Precision.

Web Security Gateways

- **Bulletproof Security**
- Integrated protection that inspects all web traffic in real time
- Ability to identify and block attacks, regardless Blocks both known and “zero-day” attacks
- Ability to protect YOUR application’s unique code
- Bi-directional security:
  - **Stop incoming attacks**
  - **Block outgoing unauthorized data**

- **Enterprise Manageability**
- Scale to handle high-volume enterprise application traffic
- Global AND Granular adminstration and delegation for complex apps
- Support for SSL
- Hot Failover and HA
- Minimal integration and configuration

TEROS™
Protect With Precision.

Web Security Gateways

- **Real-Time Protection from Malicious Attacks within Web Data Path**
  - **Assures the performance and uptime of web apps**
  - **Eliminates all classes of application attacks**
  - **APMs Protects private data (credit card numbers, social security numbers, account numbers, etc.)**
  - **Eliminates web site defacement**
  - **Enables Security and Privacy Regulation Compliance**
  - **Simple to deploy security appliance**

TEROS™
Protect With Precision.

Case Study-State Medicare Org

- **The Problem**
  - Online Medicare Claims Processing Application
  - Private health data protected by HIPAA
  - Realized only app code was protecting this data
  - Primary concern was enforcing specific policy and the ability to audit
  - Required SSL & Performance
- **The Solution**
  - APS HA with SSL
  - SAFEIdentity Module
  - Application logic and data are now secured
  - Security is auditable and uniform
  - Complete compliance with HIPAA requirements for private data protection

TEROS™
Protect With Precision.

HIPAA - References

http://aspe.os.dhhs.gov/admnsimp	Department of Health and Human Services
http://www.hcfa.gov	Health Care Financing Administration
http://ncvhs.hhs.gov	National Committee on Vital and Health Statistics
http://www.wedi.org	Workgroup for Electronic Data Interchange web site. Site includes information on EDI in the health care industry, lists of conferences and other resources.
http://www.afehct.org	Association for Electronic Healthcare Transactions
http://www.ahima.org	American Health Information Management Association
http://www.ehnac.org	The Electronic Healthcare Network Accreditation Commission
http://www.hipaadvisory.com	General HIPAA Information Site
http://www.hipaacomply.com	General HIPAA Information Site