Fifth National HIPAA Summit

HIPAA Privacy and Security Assessments in Health Care Web Sites

Suzy Buckovich, JD, MPH; Jere McLaurin
IBM HIPAA National Practice
sbuckovi@us.ibm.com;   jmclauri@ibm.com

Craig Fagin
NASCO Director of eBusiness
cfagin@nasco.com

Agenda

- □ Background on NASCO and eBusiness Strategy
- □ Overview of Health Care Benefits Online (HCBO) Website
- □ Typical Website Assessment Analysis
- □ Challenges
- □ Lessons Learned

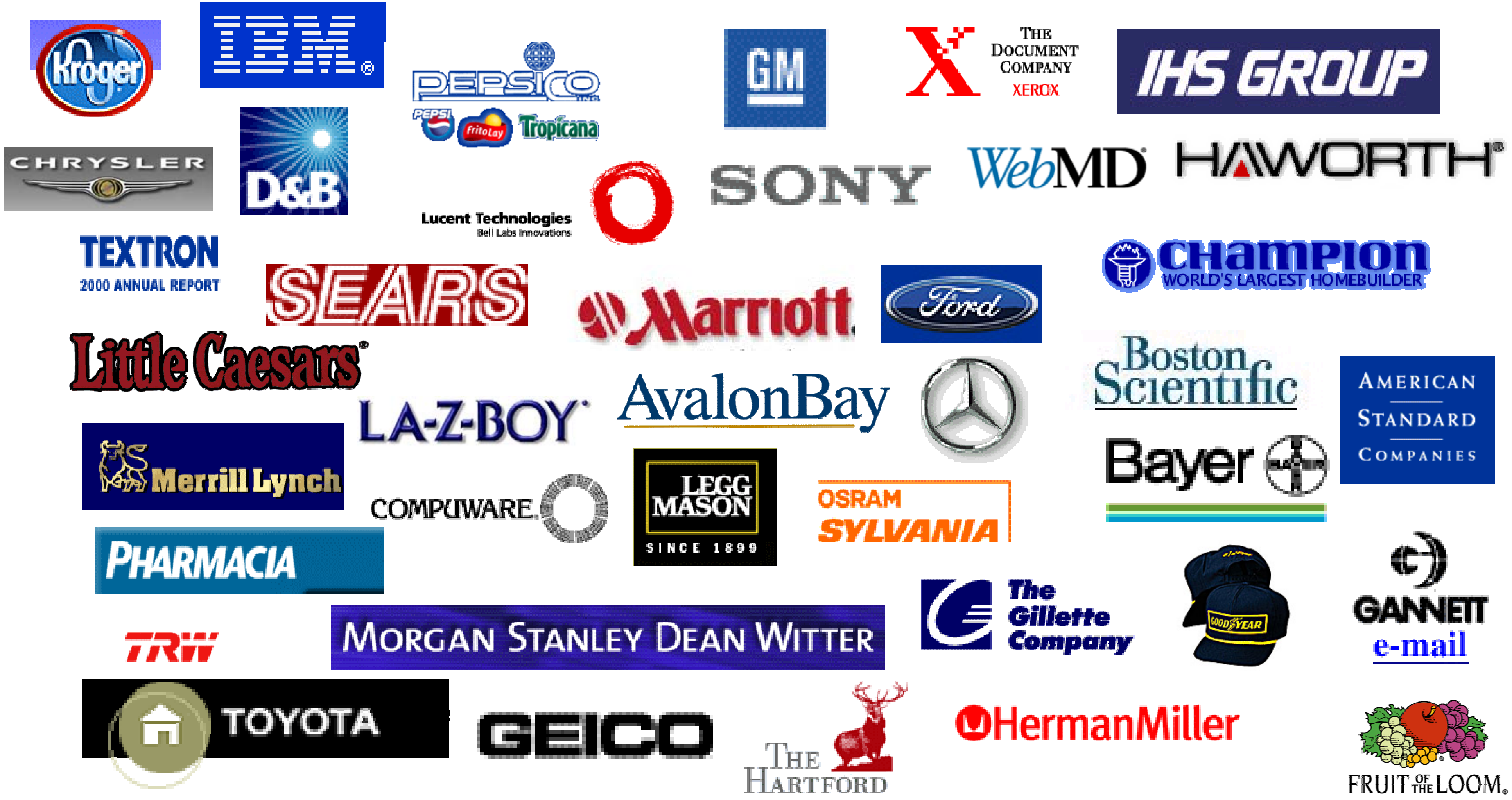
NASCO is a service company providing IT solutions to Blue Cross and Blue Shield companies

- We provide claims processing services which specialize in complex health benefits programs for large, national employers.

- We were founded in 1987 by four major BCBS companies
  - Anthem BCBS, Empire BCBS, Horizon BCBS of New Jersey, BCBS Michigan

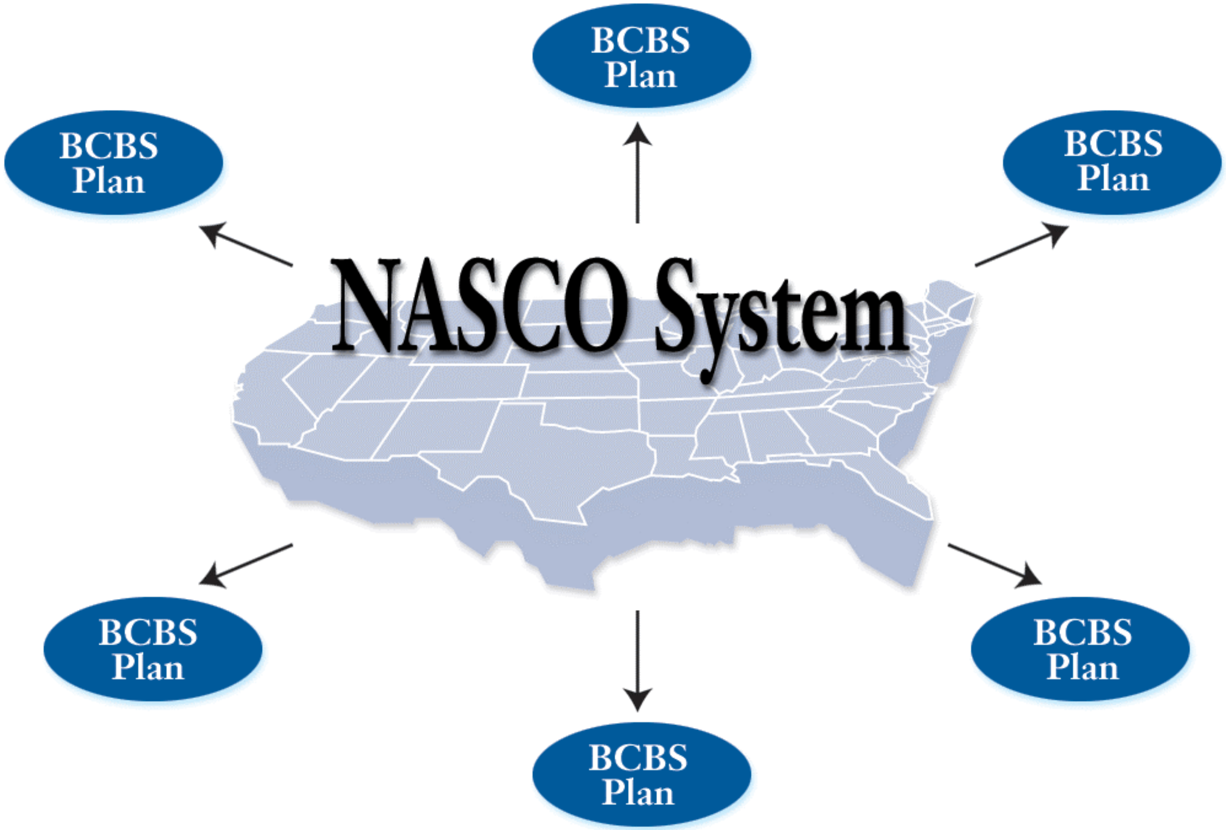
- We support many health industry products
  - Traditional indemnity plans
  - Preferred provider plans (PPO)
  - Point of service plans (POS)
  - Medicare supplemental plans
  - Vision, dental, hearing benefit programs

Using the NASCO platform, the Blues service more than 1200 multi-state employers



NASCO's business model is unique to the Blues

A national account has employees in many BCBS Plan areas



Employees' claims are adjudicated consistently and accurately no matter where they live, work or travel.

NASCO is the single largest processor for national accounts for the BCBS Plans

e-business

In 2002, we will

□ process 86,000,000 health claims

□ for nearly 7,000,000 BCBS members

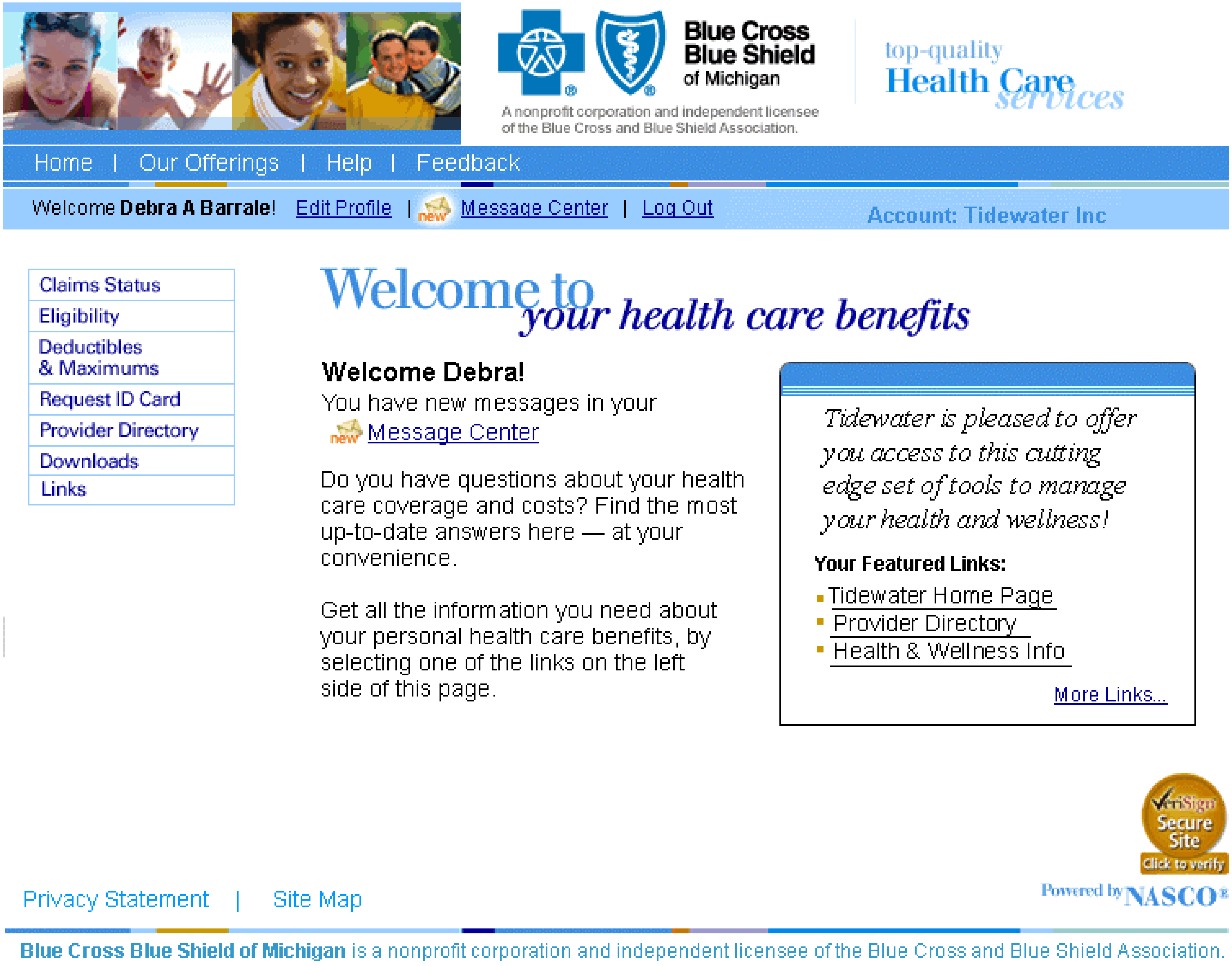
□ and pay $9,000,000,000 in covered benefits

NASCO’s eBusiness Strategy

- ❑ Two major goals:
  - Enable Internet self-service for members and accounts
  - Provide BCBS Plans with a B2B solution to access their national account data on NASCO

Both would result in greater efficiencies and improved user satisfaction

Health Care Benefits Online (hcbo.com)



Blue Cross Blue Shield of Michigan

A nonprofit corporation and independent licensee of the Blue Cross and Blue Shield Association.

top-quality Health Care services

Home | Our Offerings | Help | Feedback

Welcome **Debra A Barrale**! Edit Profile | new Message Center | Log Out

Account: Tidewater Inc

- Claims Status
- Eligibility
- Deductibles & Maximums
- Request ID Card
- Provider Directory
- Downloads
- Links

Welcome to *your health care benefits*

Welcome Debra!

You have new messages in your new Message Center

Do you have questions about your health care coverage and costs? Find the most up-to-date answers here — at your convenience.

Get all the information you need about your personal health care benefits, by selecting one of the links on the left side of this page.

Tidewater is pleased to offer you access to this cutting edge set of tools to manage your health and wellness!

Your Featured Links:

- Tidewater Home Page
- Provider Directory
- Health & Wellness Info

More Links...

VeriSign Secure Site Click to verify

Privacy Statement | Site Map

Powered by NASCO®

Blue Cross Blue Shield of Michigan is a nonprofit corporation and independent licensee of the Blue Cross and Blue Shield Association.

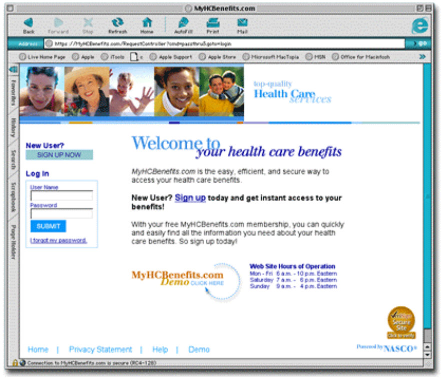
HCBO Features

Current Member Functions:

- •Online registration
- •View claims status and claims details
- •View accumulated deductibles/out-of-pocket maximums
- •View eligibility information
- •View/Print Provider directory
- •View Medicare claims and eligibility information
- •View other insurance info
- •Edit user profile
- •Request ID Cards
- •Forms Download
- •Plan and Account Specific Links

Planned Member Functions:

- •View High Level Benefits – 2002
- •View Detailed Benefits - 2003
- •View/Update COB - 2002
- •View EOBs – 2002 (under HIPAA review)
- •Consent Management – 2003
- •Customer Service Communication - 2002



New User?

Log In

I forgot my password.

Welcome to your health care benefits

MyHCBenefits.com is the easy, efficient, and secure way to access your health care benefits.

New User? Sign up today and get instant access to your benefits!

With your free MyHCBenefits.com membership, you can quickly and easily find all the information you need about your health care benefits. So sign up today!

Web Site Hours of Operation

Mon - Fri	6 a.m. - 10 p.m. Eastern
Saturday	7 a.m. - 6 p.m. Eastern
Sunday	9 a.m. - 4 p.m. Eastern

Connection to MyHCBenefits.com is secure (RC4-128)

Customer Service Rep:

- •Reset member password
- •Log in as member
- •Help member navigate through site
- •Member Communication

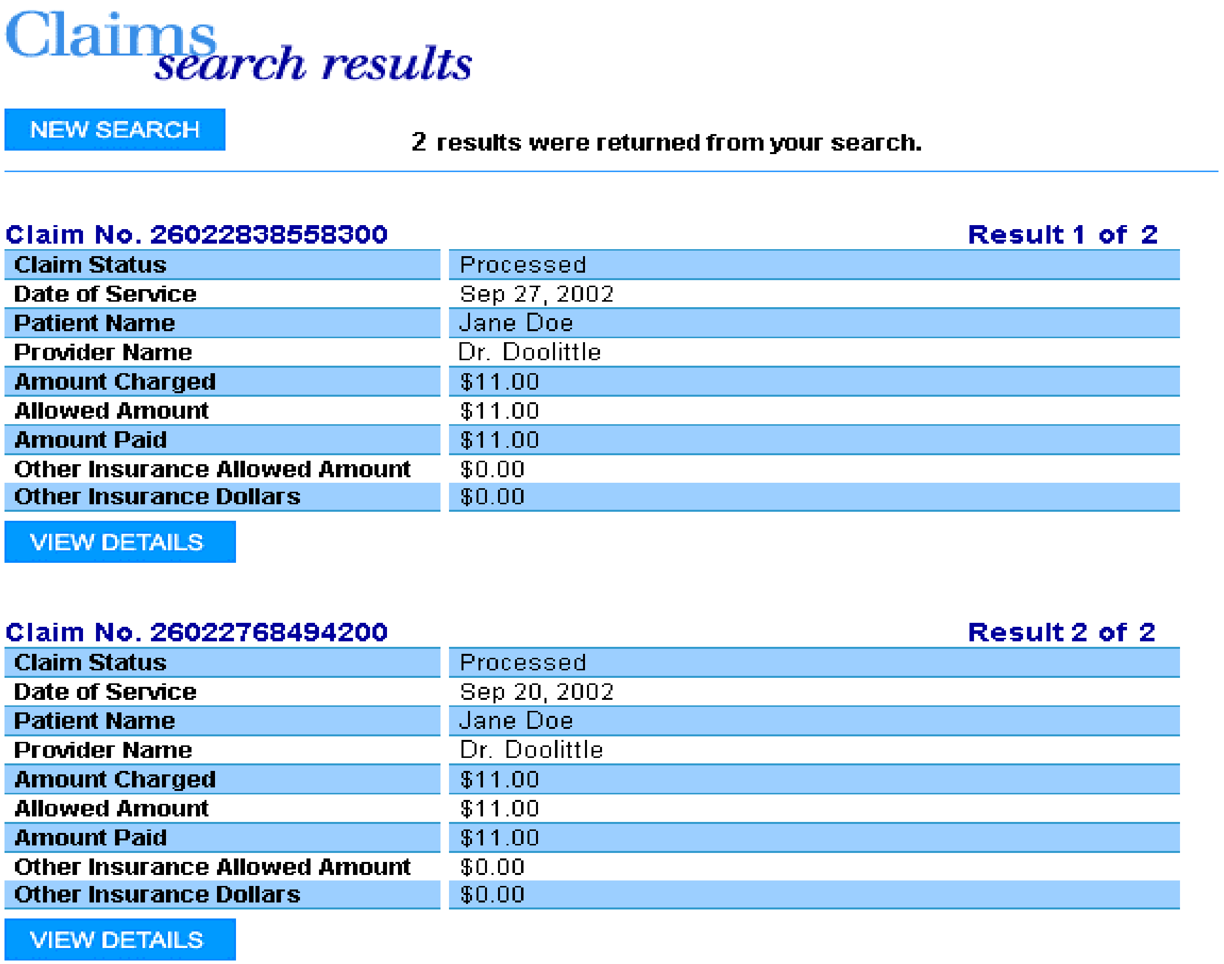
Plan Admin:

- •Site usage reports
- •Site feedback reports
- •Define user access
- •Define account features
- •Select Plan logo
- •Add new accounts
- •Member Communication

Account HR Rep:

- •Eligibility
- •Request ID card
- •Provider Directory
- •Download Forms
- •Plan and Account Specific Links
- •Update Address/Dependent - 2002
- •View High Level Benefits - 2002
- •View Detailed Benefits - 2003

Claims



Claims search results

2 results were returned from your search.

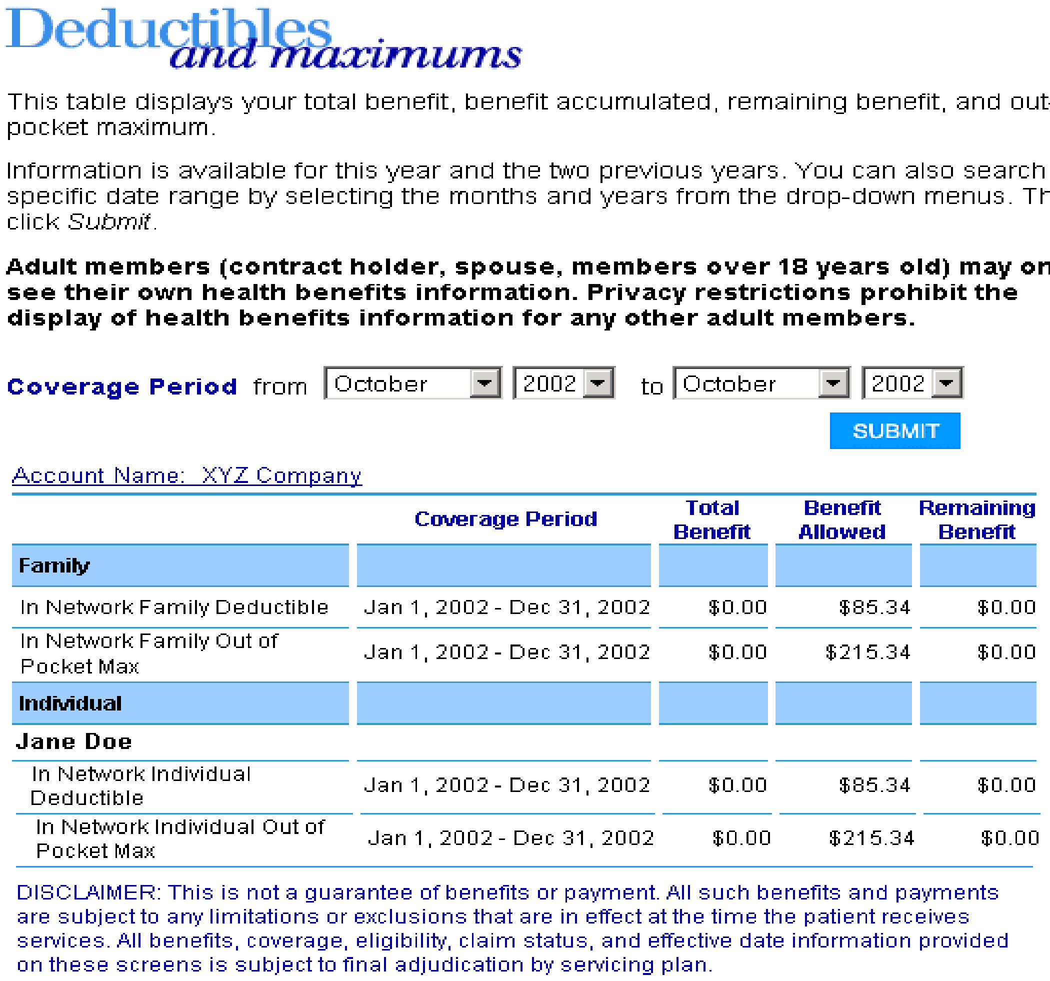
Claim No. 26022838558300 **Result 1 of 2**

Claim Status	Processed
Date of Service	Sep 27, 2002
Patient Name	Jane Doe
Provider Name	Dr. Doolittle
Amount Charged	$11.00
Allowed Amount	$11.00
Amount Paid	$11.00
Other Insurance Allowed Amount	$0.00
Other Insurance Dollars	$0.00

Claim No. 26022768494200 **Result 2 of 2**

Claim Status	Processed
Date of Service	Sep 20, 2002
Patient Name	Jane Doe
Provider Name	Dr. Doolittle
Amount Charged	$11.00
Allowed Amount	$11.00
Amount Paid	$11.00
Other Insurance Allowed Amount	$0.00
Other Insurance Dollars	$0.00

Deductibles/Maximums



Deductibles and maximums

This table displays your total benefit, benefit accumulated, remaining benefit, and out-of-pocket maximum.

Information is available for this year and the two previous years. You can also search for a specific date range by selecting the months and years from the drop-down menus. Then click *Submit*.

Adult members (contract holder, spouse, members over 18 years old) may only see their own health benefits information. Privacy restrictions prohibit the display of health benefits information for any other adult members.

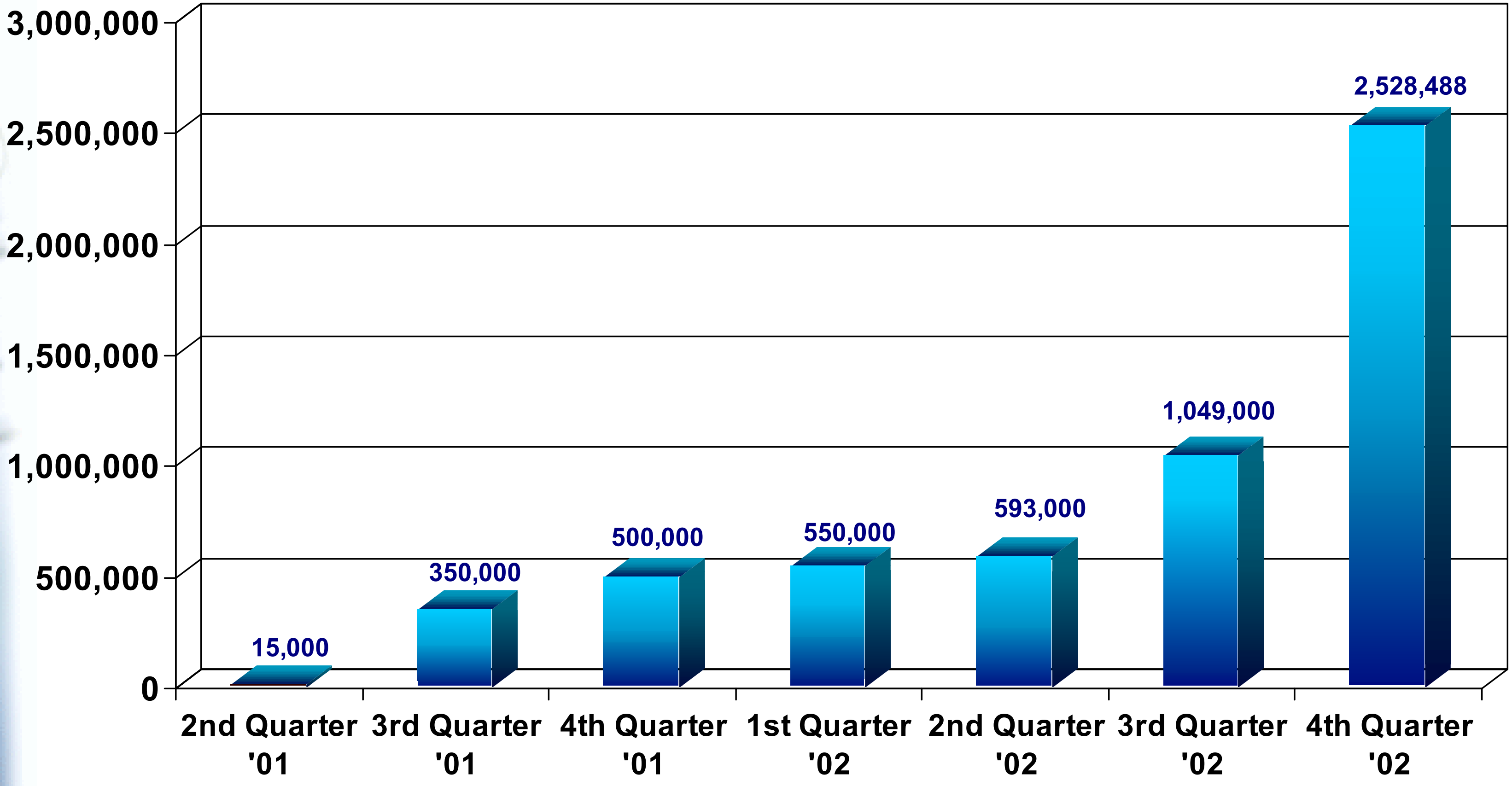
Coverage Period from October 2002 to October 2002

Account Name: XYZ Company

	Coverage Period	Total Benefit	Benefit Allowed	Remaining Benefit
Family				
In Network Family Deductible	Jan 1, 2002 - Dec 31, 2002	$0.00	$85.34	$0.00
In Network Family Out of Pocket Max	Jan 1, 2002 - Dec 31, 2002	$0.00	$215.34	$0.00
Individual				
Jane Doe				
In Network Individual Deductible	Jan 1, 2002 - Dec 31, 2002	$0.00	$85.34	$0.00
In Network Individual Out of Pocket Max	Jan 1, 2002 - Dec 31, 2002	$0.00	$215.34	$0.00

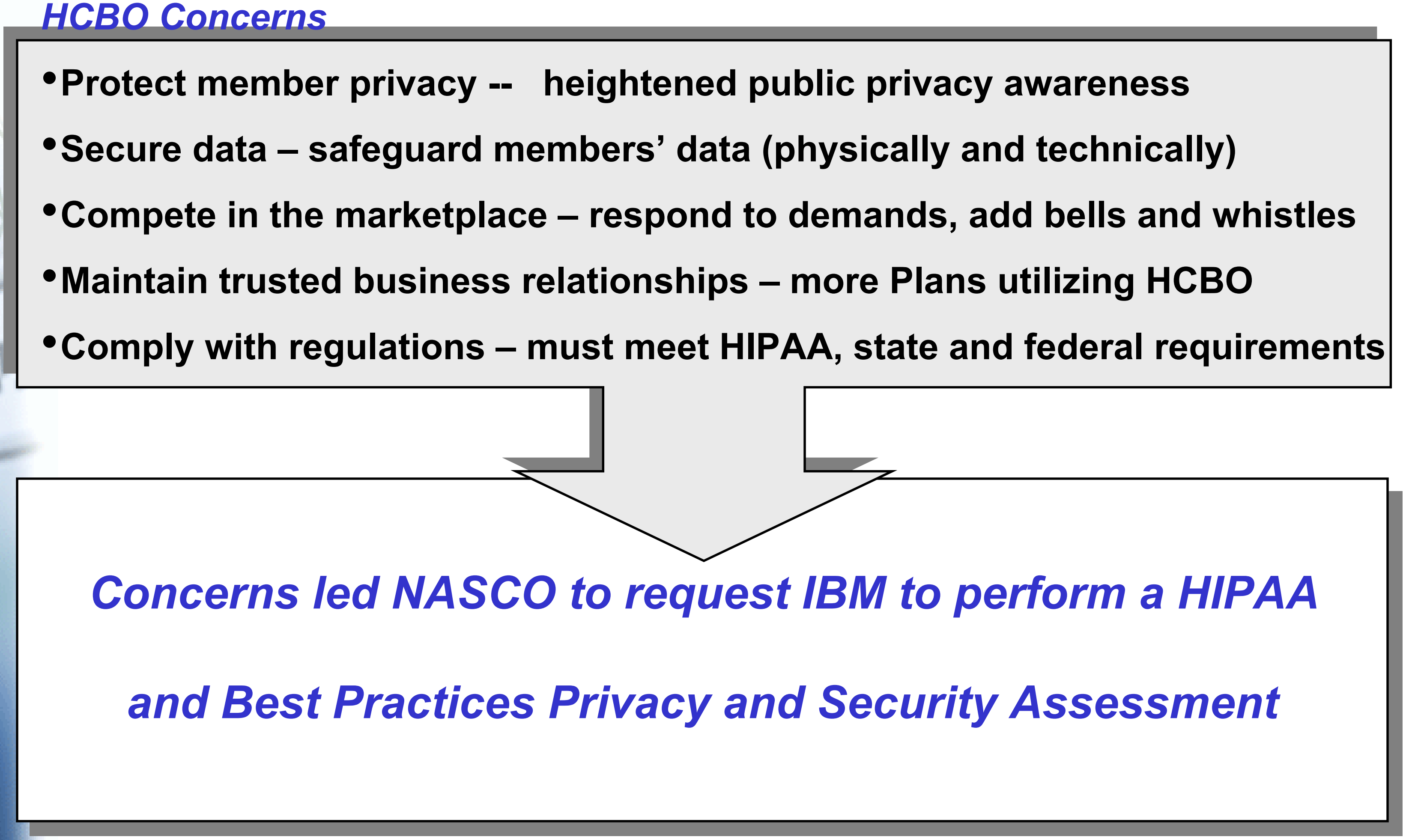
DISCLAIMER: This is not a guarantee of benefits or payment. All such benefits and payments are subject to any limitations or exclusions that are in effect at the time the patient receives services. All benefits, coverage, eligibility, claim status, and effective date information provided on these screens is subject to final adjudication by servicing plan.

BCBS Plans are deploying the Internet capability to their accounts on a regular basis



HCBO Assessment

HCBO Concerns



- Protect member privacy -- heightened public privacy awareness
- Secure data – safeguard members' data (physically and technically)
- Compete in the marketplace – respond to demands, add bells and whistles
- Maintain trusted business relationships – more Plans utilizing HCBO
- Comply with regulations – must meet HIPAA, state and federal requirements

Concerns led NASCO to request IBM to perform a HIPAA and Best Practices Privacy and Security Assessment

Overview of Assessment Approach

Privacy Online Statement

- Review statement
- Review information collection and release practices
- Review privacy and security practices (web-related) for inconsistencies
- Designate owner and create review process

Policies and Procedures

- Review privacy and security policies and procedures
- Review terms and uses
- Review contractual agreements

Privacy

- Identify PHI
- Review privacy practices
- Review business rules and design requirements

Security

- Review security controls
- Review access privileges
- Review HCBO security requirements

Features

- Review current and planned features
- Review feature design process
- Review branding issues

Success Factors

- *Management buy-in*
- *Cross functional interviews*
- *Documented requirements*
- *Utilized iterative process*
- *Incorporated usability analysis*

Privacy Online Statement Checklist

- □ Describe information collection practices?
- □ List type and intended use of information collected?
- □ Offer any individual choices? (opt-in, opt-out, etc.)
- □ Provide contact for web site privacy statement questions?
- □ Describe information sharing practices?
- □ Describe security controls?
- □ Use of Cookies?
- □ Services limited to US?
- □ Use of profiling?
- □ Target services to children under 13?
- □ Link to other sites? (provide notice to user)
- □ Outline user responsibilities? (i.e., to maintain privacy)
- □ Include last revised date?

Privacy Analysis Checkpoints

- □ Documented privacy P&Ps?
- □ Free text fields where PHI can be entered?
- □ Expectations by members? (return emails, medical answers, etc.)
- □ Links to other web sites? (notification of leaving site?)
- □ Access Controls?
- □ Posting of PHI?
- □ Access rights/privileges?
- □ Review of state laws?
- □ Use of special class of health information? (substance abuse, mental health, etc.)
- □ Emailing PHI?

Security Analysis Checkpoints

- ❑ Is security involved in requirements phase?
- ❑ Logging in place?
- ❑ Has intrusion detection been conducted?
- ❑ Encryption used for open networks?
- ❑ Documented internal security practices?
- ❑ User authentication methods (ex., 2 or 3 party)?
- ❑ Logical location of servers?
- ❑ Access control?
- ❑ Practices consistent with privacy statement?
- ❑ Business continuity and continuity plan?

Feature Analysis Checkpoints

Does the Feature Involve the Following?

Privacy

- Free text fields?
- The use or display of PHI?
- HIPAA individual rights?
- Links to other health sites?
- Links to health risk tools?
- State or federal regulations?
- Emailing PHI?
- Collection of PHI?
- Incorporated in pre-design phases?

Security

- Access to new user groups?
- Additional passwords?
- New access for existing users?
- Cookies?
- Audit trail requirements?
- Encryption?
- Incorporated in pre-design phases?

Policies

- Alignment with Terms and Uses?
- Alignment with Online Statement?
- Alignment with Contracts?
- New Procedures?
- Minimum Necessary Standard?
- Branding Issues?

Remember to assess branding

Sample Feature Assessment Tool

Features	Description	Current Feature	Planned Feature 2002	Who Can Access	Privacy Concern	Security Related Concern	Policy Impact	System Impact	Recommendation / Comments
User Registration	Allows user to sign-up for online access to benefits info; user identifed by contract # and DOB, then user creates their profile with user name, password, passwrod hint and e-mail address	X		CH, AD, HR, PA		X	X	X	Policy: Develop written policy for Terms and Conditions Agreement for new users to accept T&C prior to allowing them to set up profile System: Accommodate requirements for new users to accept T&C prior to allowing them to set up their user profile.

Assign Post Assessment Owners

Recommendation Category	Owner/Team	Completion Date
1. Revise privacy online statement and review regularly		
2. Address feature concerns (both privacy and security)		
3. Revise and implement usability recommendations		
4. Determine branding message		
5. Develop feature review criteria and feature planning process		
6. Revise policies and procedures		
7. Involve legal counsel as necessary		
8. Designate security and privacy team to work with design team		

Typical Industry Findings

Privacy Statement

- ➢Inaccuracies – practices do not reflect description
- ➢No designated owner for maintenance
- ➢No formal review process when practices change
- ➢No designated contact person

Security

- ➢No formal documented policies and procedures
- ➢Security requirements not developed before design
- ➢Server functions not adequately separated
- ➢No intrusion detection performed
- ➢Lack of audit controls
- ➢Limited emergency response procedures

Features

- ➢Free text fields (PHI could be entered)
- ➢User authentication needs to be improved
- ➢Privacy and security requirements not in design
- ➢Vulnerabilities in personalized homepages, linking to other sites, health checks
- ➢Access rights not formally defined
- ➢Include option to print user Ids, passwords

Health Care Website Challenges

- ❑ Integrating privacy and security team (and requirements) and design team
- ❑ Designing bells and whistles while protecting privacy
- ❑ Balancing liability with business partners
- ❑ Determining the appropriate security controls to put in place
- ❑ Understanding roles and granting access
- ❑ Keeping the online statement current as new security or new features are added

Health Care Website Challenges

e-business

❑ Business decisions

- Incorporate HIPAA preemption?
  - Operations in multi-state vs. incorporated state
  - Minor rights, personal representatives
- Display protected health information?
  - EOBs, social security numbers
- Include individual rights?
  - Confidential communications
  - Access/copy
- Determine level of security?
  - Industry leader
  - Industry best practices
  - HIPAA as floor

Lessons Learned

❑ Critical to interlock eBusiness initiatives with HIPAA workgroups to assess impacts and incorporate regulatory requirements

❑ Don’t forget about the supporting infrastructure

❑ Don’t leave security up to the developers -- include privacy and security requirements in pre-design phases

❑ Develop privacy and security review criteria checklists as future enhancements are designed and implemented

❑ Involve legal counsel as appropriate

Lessons Learned

❑ Document business decisions

❑ Document policies and procedures and enforce

❑ Develop communication plan to stakeholders (detailing security and privacy protections)

❑ Don’t wait to assess after development, it is harder than you think

❑ Review regularly

Questions?