GLBA and Privacy
October 25, 2001

John P. Fielding
Senior Counsel/Financial Services
National Association of Insurance Commissioners
Washington, DC

Gramm-Leach-Bliley Act

- Financial Services Modernization Act (P.L. 106-102)
- signed by President Clinton on Nov. 12, 1999
- Allows convergence of banking, securities and insurance industries
- “Functional Regulation”
- Title V - privacy provisions (notice and opt out)
- Requires “functional regulators” – including state insurance regulators – to enforce privacy protections

NAIC Model Regulation

- Background: 1980 and 1998 NAIC Model Privacy Acts
- Privacy Working Group formed early 2000 to address GLBA privacy
  - public hearings held
  - multiple drafts of model regulation distributed to all interested parties
  - comments received and considered
  - unanimously adopted by NAIC on Sept. 26, 2000

NAIC Model General Requirements

- Model regulation based on federal GLBA privacy regulations
- Notify consumers/customers about privacy policies
- Give them opportunity to prohibit the sharing of protected financial information with nonaffiliated third parties (opt out)
- No restrictions on sharing financial information among affiliates
- No opt out requirement for joint marketing/ servicing and “doing business” purposes

NAIC Model, Health Information - Why?

- Model regulation requires affirmative consent of consumers/customers before sharing protected health information with any parties
- GLBA changed the debate
- GLBA standard is opt-out
- Federal regulations referenced health information
- Insurers collect much more health information than other financial institutions
- Health information protections not beyond the scope of GLBA

Contentious issues

- Keep health out altogether - beyond GLBA
- If not, marketing exception only
- No need to act at all - HHS regulation forthcoming

Negotiated issues

- Streamlined
- Doing everyday business
- Avoid conflicts with HHS regulation

Health provisions

- Scope
- Who: Applies to ALL insurance licensees, not just health or life carriers.
- What Information: All health information.
- What Format: Applies to all disclosures of protected information.

What health information is protected?

- Nonpublic personal health information is protected.
- Nonpublic personal health information is health information that:
- identifies an individual who is the subject of the information; or
- with respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

Health information defined

- Health Information is information or data, except age or gender, whether oral or recorded in any form or medium, created or derived from a health care provider or the consumer that relates to:
- the past, present or future physical, mental or behavioral health or condition of an individual;
- the provision of health care to an individual; or
- payment for the provision of health care to an individual.

General Rule

- A licensee may not disclose nonpublic personal health information unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed ("opt in") or pursuant to one of the specified exceptions.

Exceptions to the General Rule

- claims administration;
- claims adjustment and management;
- detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;
- underwriting;
- policy placement or issuance;
- loss control;
- ratemaking and guaranty fund functions;
- reinsurance and excess loss insurance;
- risk management;

Exceptions to the General Rule

- disease management;
- quality assurance;
- quality improvement;
- performance evaluation;
- provider credentialing verification;
- utilization review;
- peer review activities
- actuarial, scientific, medical or public policy research;
- grievance procedures;
- internal administration of compliance, managerial and information systems;

Exceptions to the General Rule

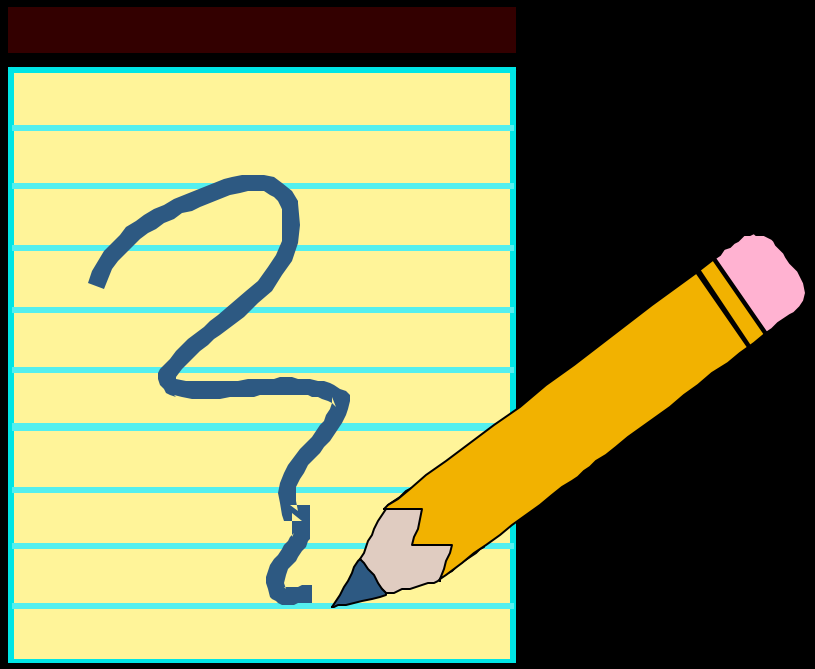
- policyholder service functions;
- auditing;
- reporting;
- database security;
- administration of consumer disputes and inquiries;
- external accreditation standards;
- the replacement of a group benefit plan or workers compensation policy or program;
- activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

Exceptions to the General Rule

- any activity that permits disclosure without authorization pursuant to the HHS health information privacy regulation;
- disclosure that is required or is one of the lawful or appropriate methods to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or services that a consumer requests or authorizes; and
- any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process.

- Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Disclosure to Third Parties/Affiliates/ Others



- The opt-in requirement applies to both affiliates and non-affiliated third parties with certain exceptions.

Notice to Consumers Regarding Confidentiality Practices

- Unlike the requirement for financial information, no notice regarding health information privacy protections is required.
- However, a valid authorization is required

Requirements for valid authorization

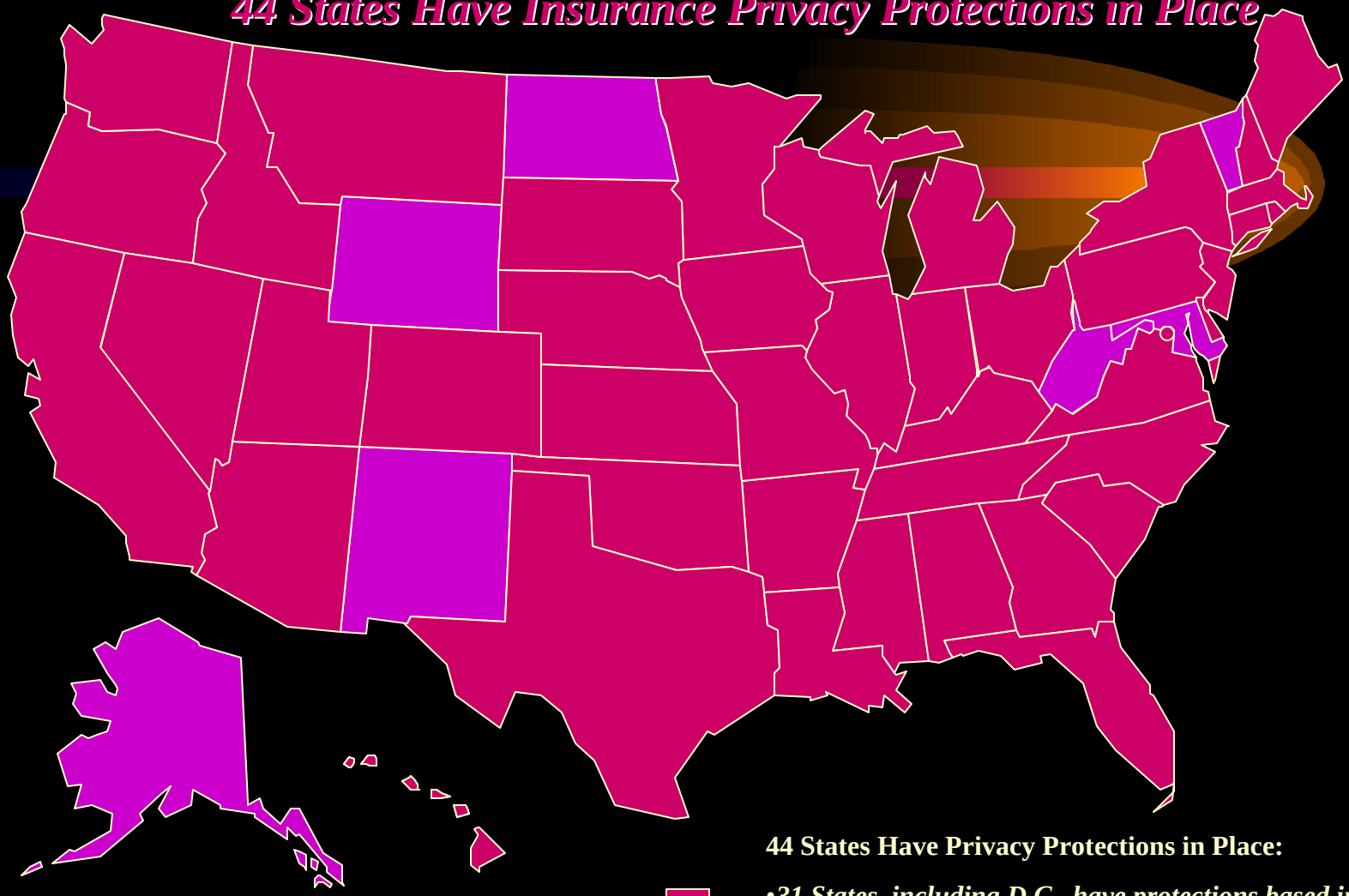
- Valid authorization to disclose nonpublic personal health information must contain the following information:
- The identity of the consumer or customer who is the subject of the information;
- A general description of the types of information to be disclosed;
- The signature of the consumer or customer who is the subject of the information, or the individual who is legally empowered to grant authority, and the date signed; and
- Notice of the length of time for which the authorization is valid; that the consumer or customer may revoke the authorization at any time; and the procedure for making a revocation.

Revocation of authorization

- An individual may revoke an authorization at any time subject to the rights of any person who acted in reliance on the authorization prior to notice of revocation

State Implementation of NAIC Model Privacy Regulation

44 States Have Insurance Privacy Protections in Place



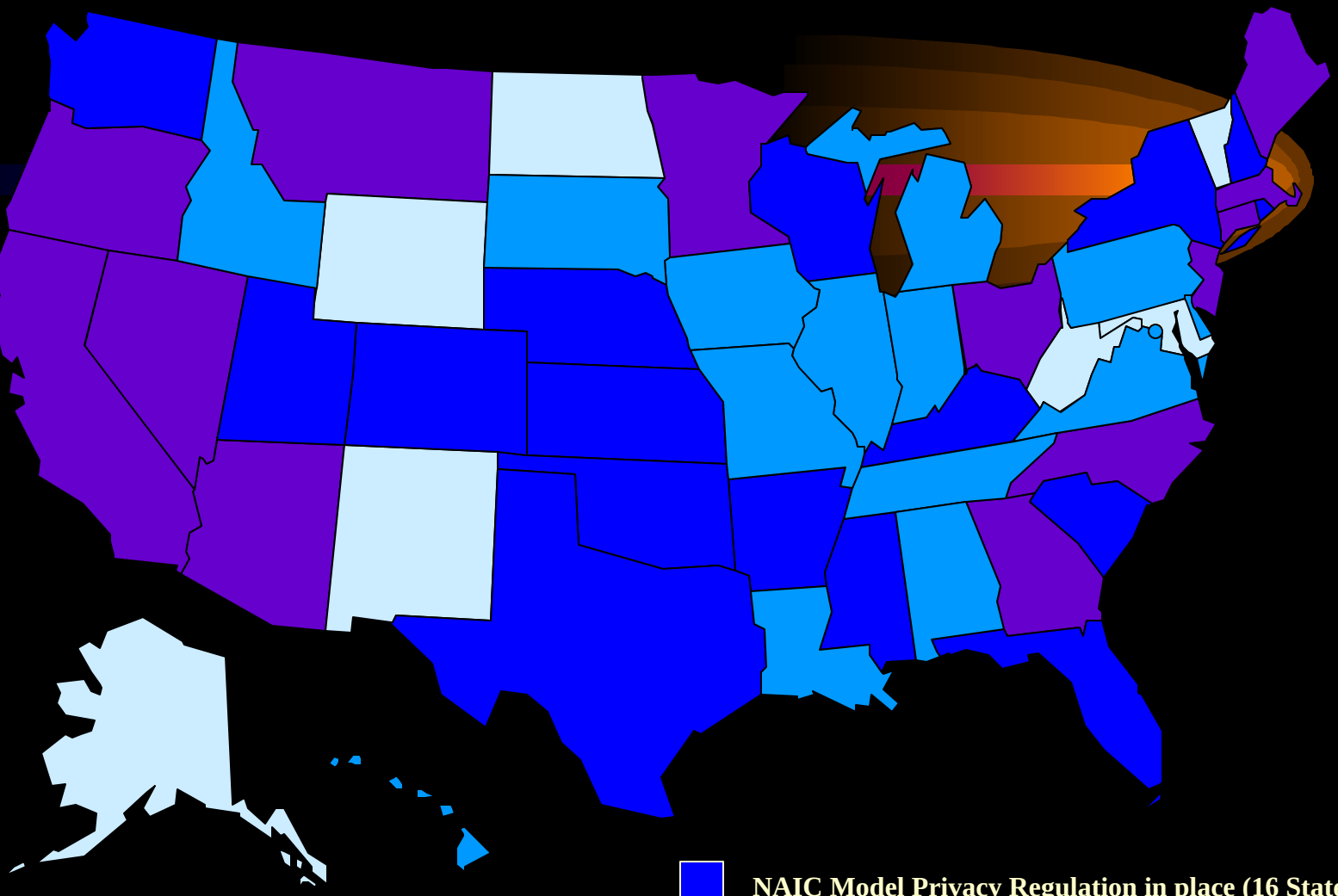
Regulations Pending (7 States)

44 States Have Privacy Protections in Place:

- ***31 States, including D.C., have protections based in whole or part on the NAIC model privacy regulation.***
- ***13 States have the 1982 NAIC model privacy act in place.***

08/21/01

State Implementation of NAIC Model Privacy Regulation



Retaining 1982 NAIC Model Privacy Act (13 States)

Regulations Pending (7 States)

NAIC Model Privacy Regulation in place (16 States)

Protections based on NAIC Model Privacy Regulation without health information provisions (15 States, including D.C.) (Several of these States have health protections in place, or will do so in the future)

08/21/01

What's Happening Now?

- NAIC Privacy Issues Working Group activities:
  - Interpretation of model/Q&A
  - Model regulation safeguarding customer information
  - Content of privacy notices
- Enforcement – Market Conduct Activities
  - Compliance survey
  - Model examination standards
  - Coordinating exams with the SEC

NAIC Privacy Web Page

- For all you need to know about the states and privacy –

  http://www.naic.org/1privacy/