

**STATE AND FEDERAL PRIVACY  
LAWS:  
NAVIGATING THROUGH THE MAZE**

Jordana G. Schwartz, Esq.

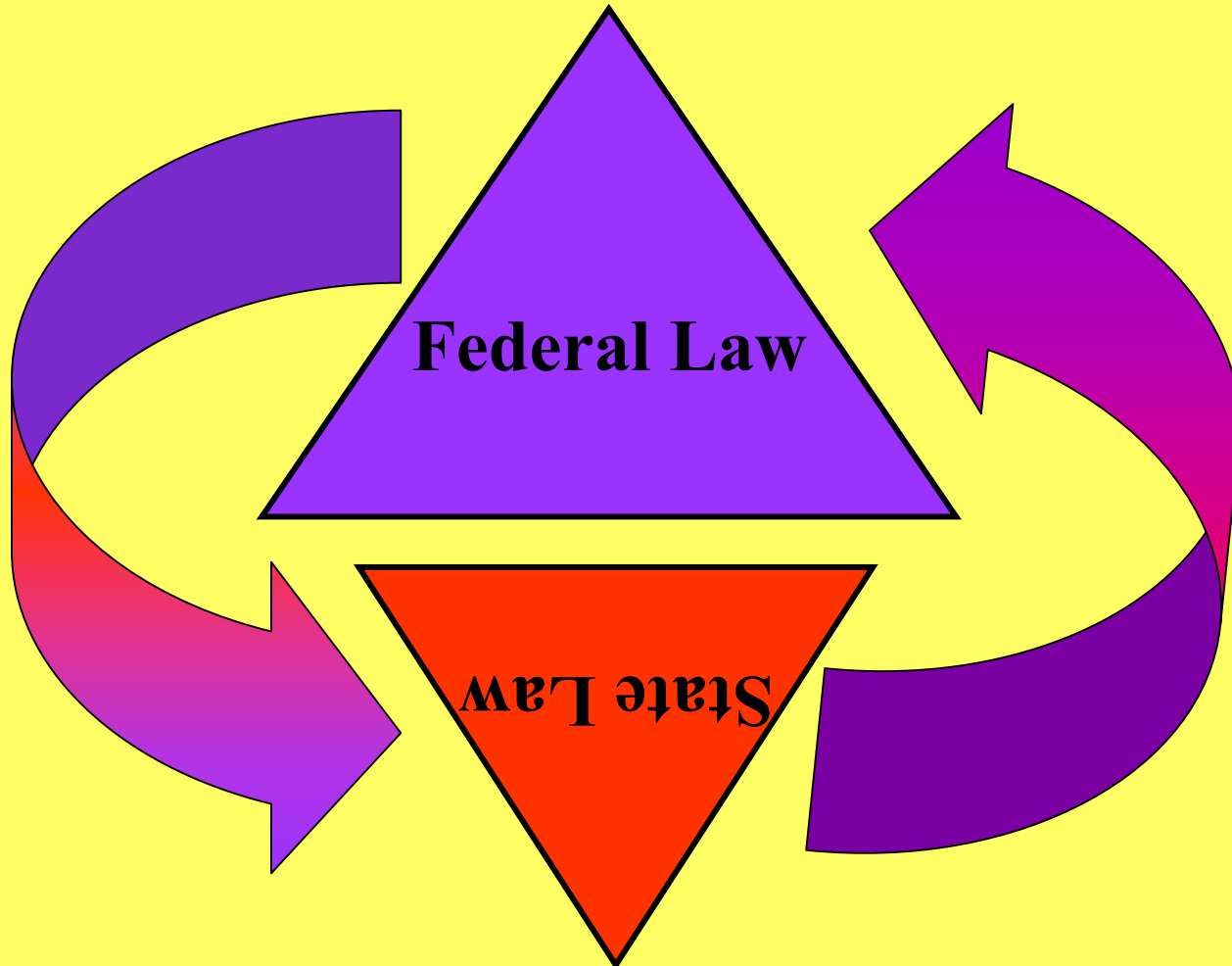
Gina M. Cavalier, Esq.

HIPAA SUMMIT VI

March 27, 2003

Sonnenschein

# HIPAA Privacy Rule Preemption of State Law



# The General Preemption Standard for the Privacy Rule

- The Privacy Rule does not preempt
  - a “provision” of
  - “state law” that
  - “relates to the privacy of individually identifiable health information,” and that is
  - “contrary to” and
  - “more stringent” than the Privacy Rule.

# Preemption

## Exceptions/Carve-outs

- **The Privacy Rule does not preempt contrary State law if:**
  - **The Secretary determines the provision of State law is necessary to:**
    - **prevent payment fraud and abuse;**
    - **ensure State regulation of insurance;**
    - **allow State reporting;**
    - **serve a compelling need related to public health, safety or welfare**
  - **The provision regulates controlled substances;**
  - **The law provides for the certain types of reporting; or**
  - **The law requires a health plan to report information for audits, program monitoring and evaluation, etc.**

# Preemption

- **Privacy Rule does not preempt**
  - **provisions of state law that are contrary and more stringent, or**
  - **provisions of state law that fall within the carve-outs/exceptions**
- **In sum:**
  - **Privacy Rule sets the federal floor**
  - **Patchwork of varying state standards**

# **“Provision” of “State Law”**

- **“Provision”**
  - **Privacy Rule requires that a preemption analysis be conducted on a provision-by-provision basis**
- **“State law”**
  - **Constitution,**
  - **Statute,**
  - **Regulation,**
  - **Rule,**
  - **Common law, or**
  - **Other state action having the force and effect of law.**

# “Relates to”

- **“Relates to the privacy of individually identifiable health information” means**
  - **the State law has the specific purpose of protecting the privacy of health information, or**
  - **affects the privacy of health information in a direct, clear, and substantial way. 45 C.F.R. § 160.202.**

# What Is “Contrary”?

- **Contrary means:**
  - **Impossible to comply with both the State and federal requirements; or**
  - **State law stands as an obstacle to the accomplishment of the HIPAA Administrative Simplification Provisions.**



# What Is “More Stringent”?

- **Six Criteria**

- (1) **Use or disclosure**

- (2) **Access or amendment**

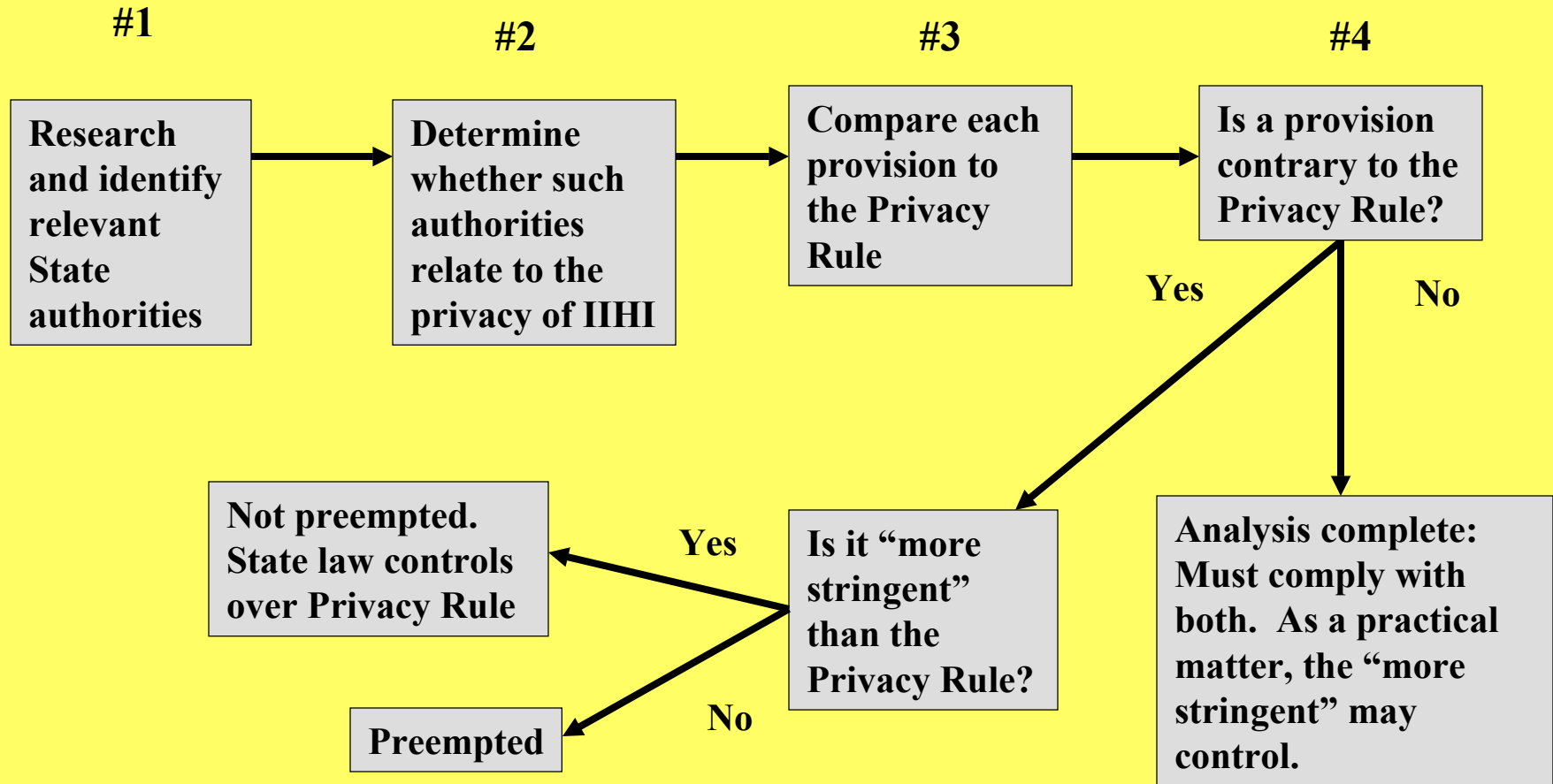
- (3) **Information to the individual**

- (4) **Form or substance of legal permission**

- (5) **Record retention and reporting**

- (6) **Greater privacy protection**

# How To Conduct A Preemption Analysis

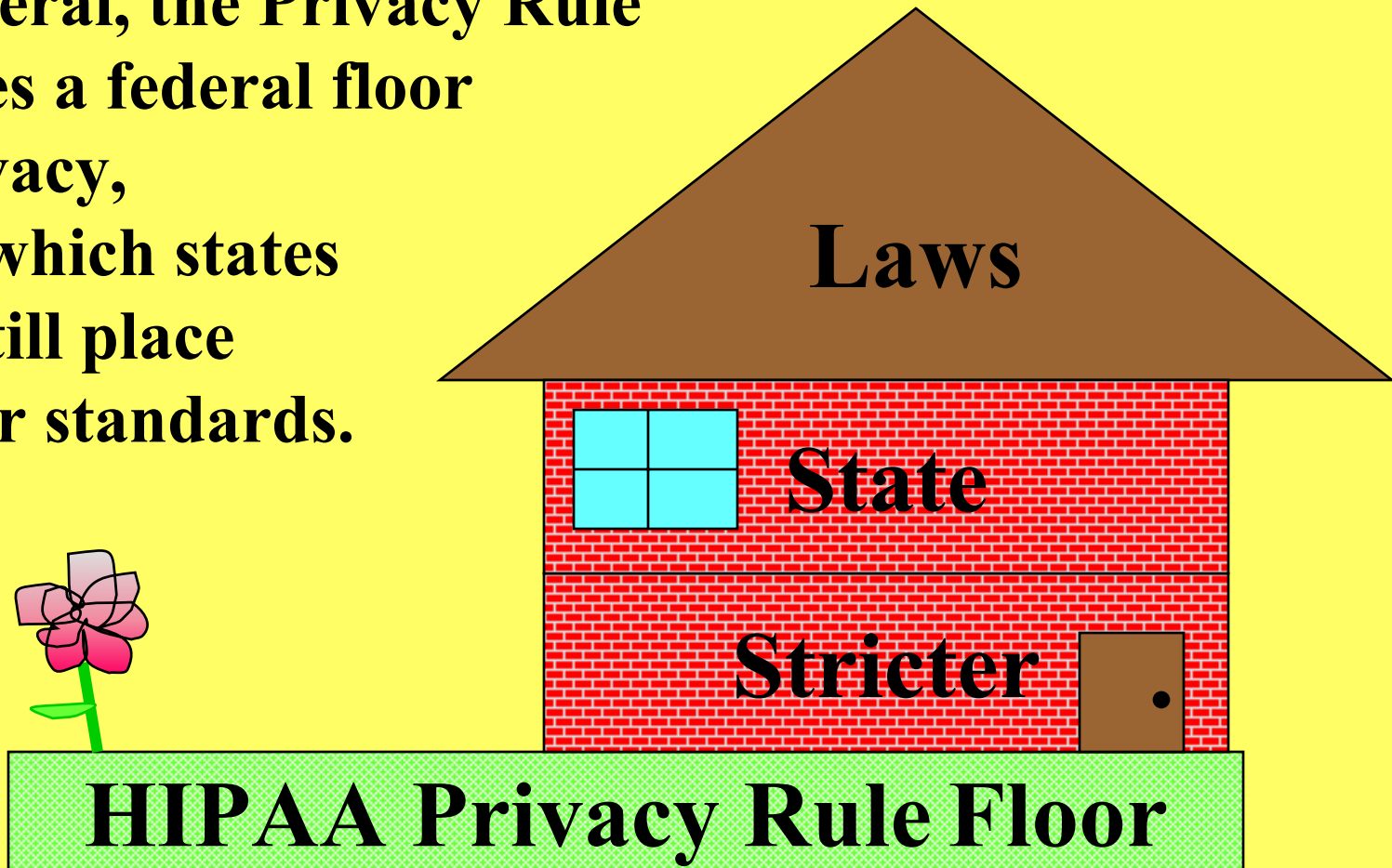


# Preemption - Example

- **State law provide that a hospital must give patients access to their information in 10 days of a request.**
- **The Privacy Rule generally requires a health care provider to grant an individual access to his or her PHI within 30 days.**
- **Relates to the privacy of health information?**
- **Contrary?**
- **Analysis ends.**
- **What to do?**

# The Effect

- In general, the Privacy Rule creates a federal floor of privacy, upon which states may still place stricter standards.



# Some Preemption Analytical Quirks

- **How to analyze:**
  - **a State law that has a limited and specified set of disclosures.**
  - **A State law that permits disclosure of protected health information where “otherwise permitted (authorized) or required by state or federal law.”**

# Current Trends in State Privacy Laws

# **Where Have We Been?**

**Entity or Condition Focused Statutes**

# **Regulation of Health Information**

- **Traditionally, State laws pertaining to the privacy of health information fell into three categories:**
  - **Insurance Regulation — NAIC Model Act**
  - **Provider Laws**
  - **Condition Specific Laws**



# **NAIC 1982 Model Act**

## **Insurance Information and Privacy Protection Model Act**

- **Establishes standards for the collection, use and disclosure of “personal information” and “medical record information” by insurance companies**
- **Contains notice, access and consent requirements**
- **17 states enacted legislation based on the Model Act, including California, Georgia, and Virginia**

# Provider Laws

- **Mainly general in focus**
- **Impose obligations on health care providers to maintain confidentiality of patient information**
  - **Florida: Fla. Stat. Ann. § 456.057**
  - **Arizona: Ariz. Rev. Stat. § 12-2292**
  - **Indiana: Ind. Code Ann. § § 16-39-5-1 through 16-39-5-3**
- **A few states have more detailed requirements**
  - **New York: N.Y. Pub. Health Law § 18**
  - **California: Confidentiality of Medical Information Act, Cal. Civ. Code § 56**
  - **Washington: Uniform Health Care Information Act, Wash. Rev. Code Ann. § 70.02.020**

# Condition Specific Laws

**Most states have condition specific laws:**

## ■ HIV and other communicable diseases

- Ariz. Rev. Stat. §§ 36-661, 664
- Ind. Code Ann. § 16-41-8-1(a)
- Fla. Stat. Ann. § 381.004

## ■ Mental Health

- Ariz. Rev. Stat. §§ 36-507, 509
- Ind. Code Ann. § 16-39-2-3 and 5
- Fla. Stat. Ann. §§ 394.451, 455

## ■ Genetic Information

- Ariz. Rev. Stat. §§ 12-2801, 2802
- Ind. Code Ann. §§ 27-28-26-1 through 11 (applies to insurers only)
- Fla. Stat. Ann. § 627.4301 (applies to insurers only)

# **Where Are We Going?**

**GLBA, HIPAA and Beyond**

# New Trends

- **There is a growing interest in privacy issues at the state level in response to the passage of GLBA (Pub. L. 106-102 signed into law on November 12, 1999)**
- **GLBA is a federal law which applies to Financial Institutions, including insurance entities**
- **Obligates states to promulgate implementing regulations applicable to insurers**

# GLBA

- **Requires all financial institutions to establish privacy policies with respect to the collection and disclosure of consumer information**
- **Requires financial institutions to disclose their privacy policies to consumers**
- **Requires financial institutions to provide their consumers with an opportunity to “opt-out” from the sharing of certain non-public personal information with nonaffiliated third parties**
- **Requires financial institutions to establish safeguards to protect the confidentiality, security and integrity of customer information**

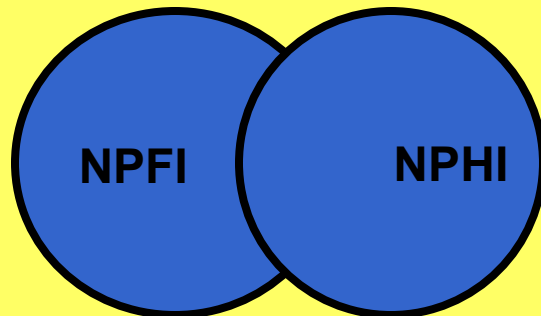
# GLBA - Impact on States

- **To date:**

- **23 States have enacted NAIC Model Privacy Regulation which meets GLBA standards**
- **13 States have enacted the financial, but not health, provisions of the NAIC Model Privacy Regulation**
- **13 States have retained the NAIC's 1982 Model Act**

# NAIC MODEL REGS

- **Separate Provisions for:**
  - **Non-public personal financial information; and**
  - **Non-public personal health information.**





# **Intersection of GLBA and the Privacy Rule**

- **NAIC Model Regulation - An entity that complies with the Privacy Rule is deemed to be in compliance with GLBA (Article V, Section 20)**
- **Result: GLBA has imposed increased administrative burdens, but has had little real impact on increasing privacy protection at the State level.**

# New Developments

- **The impending compliance date for the Privacy Rule has further increased state focus on privacy issues, both on expanding state protections and integrating them with the Privacy Rule**
- **Examples:**
  - **Texas**
  - **California**
  - **Colorado**

# Texas

- **Senate Bill 11, Effective September 1, 2001 (Codified at Tex. Health & Safety Code Ann. § 181.001 et seq.)**
- **Compliance Date - September 1, 2003**
- **To date, no regulations have been promulgated by the Texas Department of Health**
- **Builds on the requirements of the Privacy Rule, but expands definition of covered entities**
- **Privacy Rule Definition of Covered Entity:**  
“Covered Entity” means:
  - (1) a health plan
  - (2) a health care clearinghouse
  - (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter

# Texas, cont'd

**Texas Definition of Covered Entity: “Covered Entity” means any person, other than an employer, who:**

- **(A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site;**

# Texas, cont'd

- **(B) comes into possession of protected health information;**
- **(C) obtains or stores protected health information under this chapter; or**
- **(D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.**

# Texas, cont'd

**Compliance with Federal Regulations: Texas Covered Entities must comply with Privacy Rule Standards relation to:**

- **An individual's access to PHI**
- **Amendment of PHI**
- **Uses and disclosures of PHI, including requirements relating to consent**
- **Notice of Privacy protections for PHI. Tex. Health and Safety Code Ann. § 181.101.**

# Texas, cont'd

- **Information for Research:**

**A Texas covered entity may disclose PHI to a person performing health research, regardless of the source of funding of the research, for the purpose of conducting health research provided that the required consent and authorization is received.**

**Tex. Health and Safety Code Ann. § 181.101.**

# Texas, cont'd

## Repealing Legislation

- **SB 330**
- **Referred to Public Health Committee - March 5, 2003**
- **If passed, will repeal compliance with Privacy Rule and research provisions of SB 11**
- **Effective date: September 1, 2003**



# California

- **Chapter 489**
- **Passed September 12, 2002**
- **Effective until January 5, 2005**
- **Effort to integrate California laws with the Privacy Rule**
- **Creates Office of HIPAA Implementation (the “Office”)**
- **Requires state entities impacted by HIPAA to assist in determining which states laws concerning personal medical information are preempted by HIPAA and conform to all decisions of the Office**
- **Provides that any provision of State law concerning personal medical information shall not be applicable to the extent it is preempted**

# Colorado

- **Senate Bill 03-51 “Concerning Changes to State Laws In Relation to the Federal HIPAA, As Amended”**
- **Passed in Senate with Amendments, 2/11/03**
- **Introduced in House and Assigned to Health, Environment, Welfare and Institutions Committee, 2/14/03**
- **Also an effort to conform State law with the Privacy Rule**
- **Sets forth legal uses and disclosures of PHI, except in those circumstances where “authorization or an opportunity to agree or object is required by” HIPAA**

# State Agency Activity

- **Many state agencies have done their own preemption analysis, even where not legislatively directed**
- **See NYS HIPAA Website:**
  - **[www.oft.state.ny.us/hipaa/tools.htm](http://www.oft.state.ny.us/hipaa/tools.htm)**

# Predictions

**States will continue to:**

- **Respond to consumer demands to protect the privacy of the health information**
- **Attempt to integrate State privacy laws with the Privacy Rule**

# Providing Comprehensive Legal Services for the Health Care Community

**Jordana Schwartz, Esq.**

**212-768-6800**

**[jgschwartz@sonnenschein.com](mailto:jgschwartz@sonnenschein.com)**

**Gina M. Cavalier, Esq.**

**202-408-6400**

**[gcavalier@sonnenschein.com](mailto:gcavalier@sonnenschein.com)**

*Chicago Kansas City Los Angeles New Jersey New York  
Palm Beach San Francisco St. Louis Washington, DC*

**Sonnenschein**