

The Health Insurance Portability and Accountability Act (HIPAA) and Clinical/Behavioral/Community Research

UCSF Center for Aging in Diverse Communities Scientists

December 9, 2020

Steve Gregorich

Health Insurance Portability and Accountability Act (HIPAA) and Research

Common confusion about how HIPAA impacts research requirements

Potentially differing interpretations across institutions and IRBs

Within institutions, details/definitions are not always well-articulated;
Researchers, IRB members, attorneys often lack
shared definitions and concepts

This presentation will summarize

- . Some HIPAA definitions and concepts
- . Key University of California (UC) positions on HIPAA & research

Like all institutions, the UC position on HIPAA & research may evolve

Definitions & Concepts

HIPAA Privacy Rule

Protect confidentiality & security of personal health information (PHI)
arising from health care provision

. 18 HIPAA Identifiers

Names	Account numbers
Geographic subdivisions smaller than a state, Geocodes	Certificate/license numbers
Dates. All elements of dates except year, unless individual is > 89 yrs.	Vehicle identifiers/serial numbers
Telephone numbers	Device identifiers/serial numbers
Fax numbers	Web URLs
Electronic mail addresses	IP addresses
Social security numbers	Biometric identifiers
Medical record numbers	Full face photographic images
Health plan beneficiary numbers	Any other unique identifying number, characteristic, or code

Definitions & Concepts

Entities Subject to HIPAA: Covered & Hybrid Entities

Covered Entity: An organization that has to comply with HIPAA

- . *Health care provider* that conducts certain transactions in electronic form
Furnish, bill, or receive payment for health care in the normal course of business and transmit any covered transactions electronically
- . *Health care clearinghouse*, or
- . *Health plan*

Hybrid Covered Entity: UCSF is a Hybrid Covered Entity

- . A single entity that performs both covered and non-covered functions
- . Split operations: health care versus non-health care components
- . Most Privacy Rule requirements apply only to health care components
- . E.g., research labs excluded from the hybrid entity's health care components are not subject to the Privacy Rule

Definitions & Concepts

Use and Disclosure of PHI

- . When PHI is shared w/in a covered entity, that is a use of the PHI
- . When PHI is shared outside a covered entity, that is a disclosure
- . HIPAA allows use and disclosure of PHI for research purposes
Such uses and disclosures must follow HIPAA guidance and must be part of a research plan that is IRB-approved

Definitions & Concepts

Research Health Information (RHI)

According to UC, PHI-like information in a research data record constitutes Research Health Information (RHI)

Some use an equivalent label, Personally Identifying Information (PII)

Disclosure of PHI for Research Purposes

PHI becomes RHI

- . Participants each sign a HIPAA Authorization to have PHI from their medical record disclosed to an investigator for research purposes (or a waiver allowing disclosure of PHI is issued by the IRB)
- . Once the corresponding information is in the research record...
 - . it is no longer PHI subject to the HIPAA Privacy Rule
 - . it is RHI governed by the HIPAA Authorization terms & informed consent
- . The RHI data derive from voluntary participation in a study, not as a result of a healthcare provision event
- . Best practices for research involving human subjects must be held

Sharing RHI with a Covered Entity

RHI becomes PHI

When RHI from the research study is shared w/ a covered entity & entered into the existing medical record, that information —within the medical record—is PHI

This is the only way that data from a research project conducted by a non-covered entity can become PHI

However, the corresponding research data within the research database remains as RHI.

It is not PHI and is not governed by the Privacy Rule

Best Practices for Clinical/Behavioral/Community Research that is not Subject to HIPAA...

...do require

- . IRB Approval
- . Maintenance of confidentiality
- . Security of information
- . That minimum necessary information is collected
- . Separation of person-identifiable data from scientific data
- . Role-based access control for individually identifiable data elements.
I.e., access to research data elements is on a 'need to know' basis

...but, typically do not require

- . HIPAA administrative requirements for business associate agreements
- . Logging of disclosures
- . Audit trails

Summary

The label 'PHI' should be used sparingly to refer to the 18 types of identifiers that are created, received, or maintained *by a covered entity* under HIPAA (or a health care component of a hybrid covered entity)

With appropriate authorization, a covered entity may disclose PHI to a non-covered entity (e.g., research team) for research purposes.

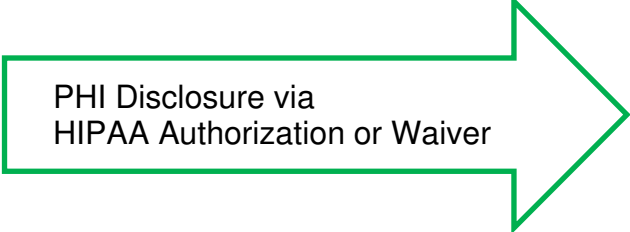
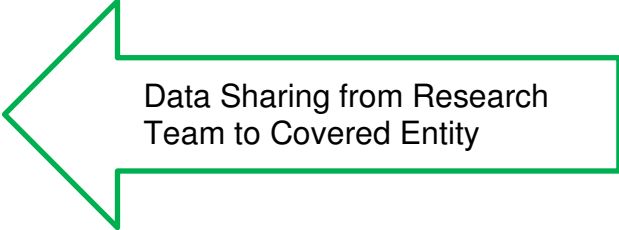
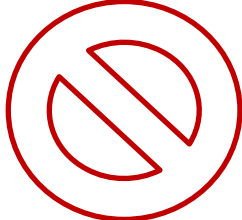
PHI becomes RHI. RHI is not subject to HIPAA

Data created & maintained by non-covered entities may be RHI.

If RHI is shared with a covered entity, then
—in the possession of the covered entity—
those same data values may constitute PHI.

RHI is not subject to the HIPAA Privacy Rule, but is subject to standard 'best practice' guidelines for research

The 18 HIPAA Identifiers: PHI or RHI?

Covered Entity e.g., Health Care Provider	Transfer of Identifying Information	Non-Covered Entity e.g., Research Team
PHI	 <p>PHI Disclosure via HIPAA Authorization or Waiver</p>	RHI
PHI	 <p>Data Sharing from Research Team to Covered Entity</p>	RHI
PHI		RHI

Q&A for Clinical/Behavioral/Community Research

Q: Is my research team/center/unit/lab considered a *covered entity*?

See the flow diagrams at the end of this slide deck. For most UCSF Clinical/Behavioral/ Community human subjects research, 'No'

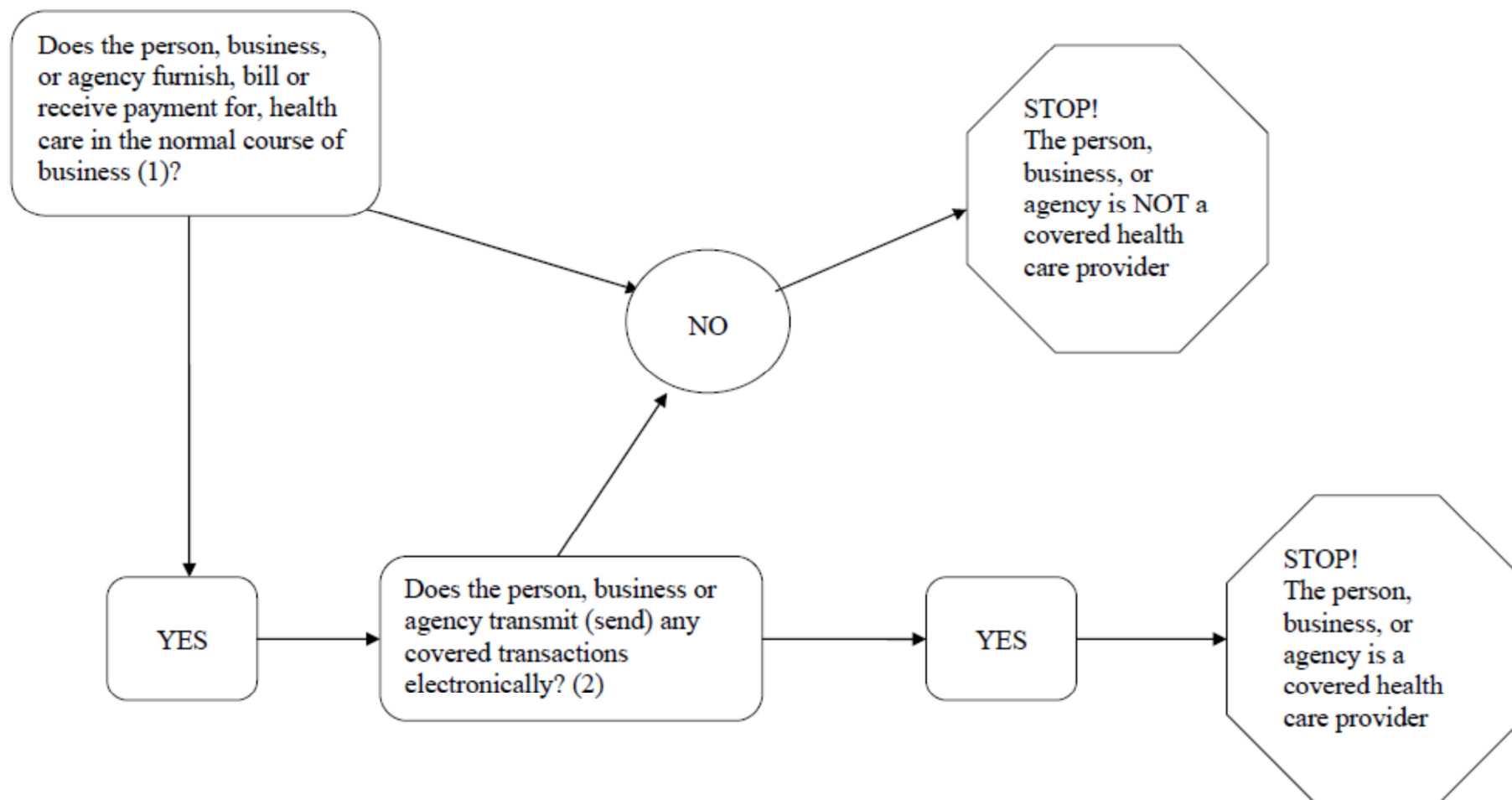
Q: Are data elements that a research project collects directly from voluntary study participants, under informed consent, considered by UC as PHI that is subject to HIPAA? No

Q. If a research project obtains HIPAA Authorizations (or a waiver) to abstract/extract PHI from the medical records of a covered entity and subsequently enter the abstracted data elements into the research data base, does UC consider the abstracted data elements in the research data to be PHI subject to HIPAA? No

Q. Does UC require the research data systems and processes used by non-covered entities to be fully compliant with HIPAA standards? No

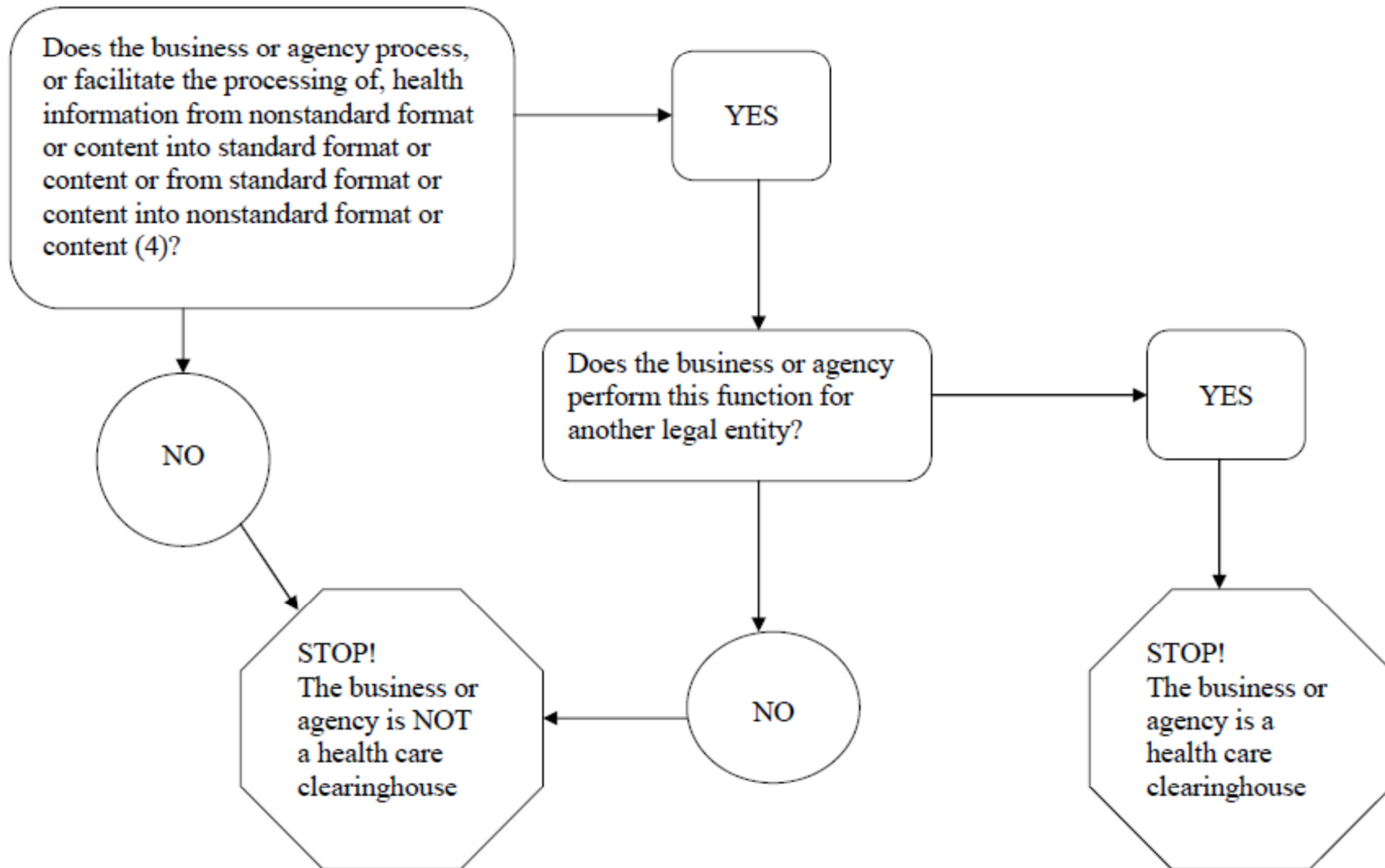
more info: <https://irb.ucsd.edu/HIPAA-Information.shtml>

Is a person, business, or agency a covered health care provider?

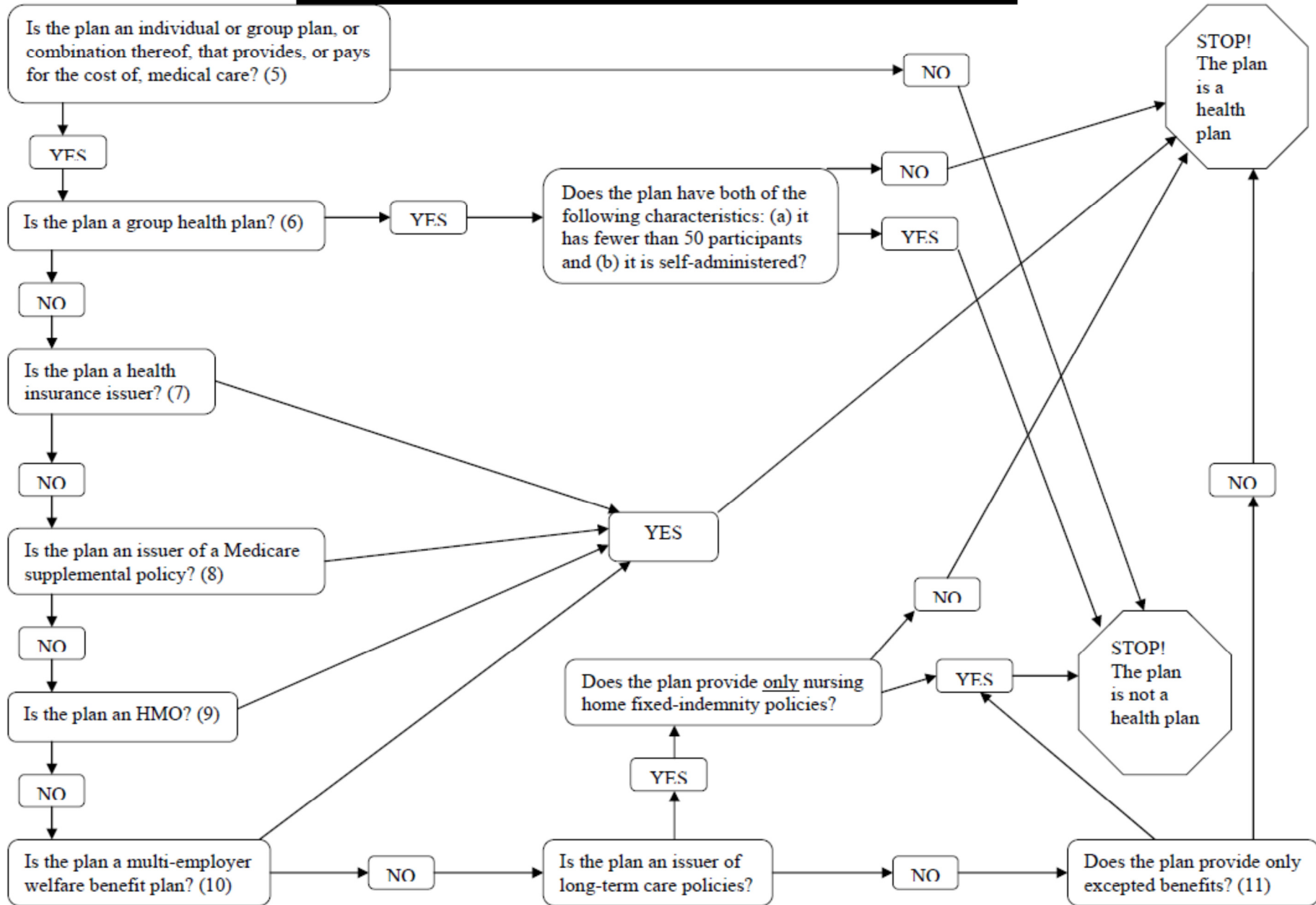


e.g., <https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf>

Is a business or agency a health care clearinghouse?



Is a private benefit plan a health plan?



Is a government-funded program a health plan?

