MEMORANDUM

To: Oregon State Bar Membership

From: Lisa Norris-Lampe
Chair, Oregon Judicial Department eCourt Law and Policy Work Group

Re: Oregon eCourt -- Opportunity for Comment on Development of Policies and Rules Related to Confidentiality and Internet Access to Court Documents

Date: August 19, 2009

As noted in Chief Judge Brewer's accompanying cover memo, in the course of developing Oregon eCourt, the Oregon Judicial Department (OJD) has been in the process of considering a variety of issues relating to the future availability of remote access to electronic court documents via the Internet. (Remote access is anticipated to be available some time during the 2011-13 biennium). To facilitate those discussions, an eCourt Law and Policy Work Group has been working for some time on the following (among other work items):

(1) the development of general guiding principles concerning the protection of confidential and sensitive information in court documents that may be available by remote access over the Internet, including general policies concerning redaction and segregation of certain information;

(2) the development of a proposed model of external user access to electronic versions of many court documents via the Internet;

(3) within the structure of that proposed user access model, the development of a related model of remote access to particular documents, both as to particular case types and across case types; and

(4) the preparation of a draft Uniform Trial Court Rule (proposed new chapter 22) relating to protected information in court documents, redaction, segregation, and remote access to electronic documents (among other topics).

The Law and Policy Work Group has completed a series of recommendations relating to the first, second, and fourth items listed above (work on the third item is ongoing). Those recommendations were presented to the joint OSB/OJD eCourt Task Force on August 11, 2009. The Bar, in turn, is coordinating distribution of the materials to its membership, via this memo, for further consideration and comment.

Attached to this memo, you will find four separate documents (listed as Sections I, II, III, and IV), all developed by subgroups of the Law and Policy Work Group and approved for distribution by that Work Group and the OJD eCourt leadership, as follows:

(I) Foundational Principles and Tools: This document provides background information for the User Access Matrix materials summarized in item II, below. As part of its deliberative process, a subgroup of the Law and Policy Work Group developed this document to serve as an orientation tool as the group worked through issues concerning remote access to electronic documents (including the difference between electronic documents generally and those electronic court documents that will be available through remote access via the Internet).

(II) Proposed User Access Recommendations: This document consists of two parts: (1) a discussion of the Law and Policy Work Group's proposed user access recommendations; and (2) a proposed User Access Matrix (the matrix appears at the end of this document). This document defines in general terms the Law and Policy Work Group's recommendations for remote user access, via the Internet, to case documents that will be stored in electronic form in the OJD's Electronic/Enterprise Content Management (ECM) system. The Work Group anticipates that the matrix will apply to documents in the circuit courts and the appellate courts, at the point in time when court documents become available via the Internet.

(III) Redaction-Segregation Subgroup Recommendations: This document is a companion to the User Access Matrix document. Several different subgroups of the Law and Policy Work Group are working on issues concerning confidentiality and remote access to electronic documents; much of the preliminary work (including the draft UTCR chapter 22, item IV, below) has been completed by the Redaction-Segregation Subgroup. As part of its decision-making process, the Redaction-Segregation Subgroup prepared a series of general recommendations that apply across case types, set out in this document.

(IV) Draft UTCR chapter 22: The purpose of draft UTCR chapter 22 is to establish a process that will facilitate remote access to electronic court documents via the Internet. The draft UTCR is very much a work in progress. The Redaction-Segregation Subgroup (which drafted the UTCR) is satisfied that the draft generally embodies how remote public access to the ECM system will work. The draft is “tentative,” however, in that it now is being used by other subgroups of the Law and Policy Work Group that are addressing more particular questions concerning documents in certain types of cases (such as civil generally, criminal generally, domestic relations, criminal, probate, juvenile, and so on). Periodically, as those subgroups complete their work, the Redaction-

Segregation Subgroup will revisit draft UTCR chapter 22 and determine whether and to what extent the draft should be modified to accommodate peculiarities of the various case types.

Both the Law and Policy Work Group and the OSB/OJD eCourt Task Force encourage the Bar membership to review the attached materials and to provide feedback in the manner directed by the Bar. Following the feedback period, the Law and Policy Work Group will consider all feedback that is received for incorporation into further recommendations to the OJD eCourt leadership.

Thank you in advance for your assistance and participation as we continue to work together to develop this important aspect of Oregon eCourt.

Law & Policy Committee

Confidential Information Workgroup
Foundational Principles and Tools
June 4, 2009

1. Public Access

If a court file is maintained exclusively in electronic form, anything in the court file must be available to the parties, the court, and the public on the same terms as the paper file is now available, even if that availability is limited to a terminal at a kiosk physically located at the courthouse. Remote electronic access may be limited.

Parties, the court, and the public should have as much access as possible to court files stored electronically, subject to limitations as necessary:

- To comply with laws protecting confidentiality of information;
- To protect the legitimate privacy concerns of parties and other affected persons that are heightened because of the powerful search capabilities of information stored electronically in a database

2. Ease of Implementation

To the extent practicable, whatever steps must be taken to protect confidential information should not require more work by parties and court staff than now required and, if possible, should require less work.

3. Burden

It is the responsibility of parties to take steps to ensure the nondisclosure of protected information with respect to papers filed by parties.

- It is the responsibility of each court to take steps to ensure the nondisclosure of confidential information with respect to documents created by the court (principally notices, letter opinions, orders, judgments).
- It is the responsibility of the Chief Justice/Judicial Department to provide the tools whereby parties and courts can protect confidential information stored

electronically, which includes information contained in documents filed by another party.

- OJD cannot possibly anticipate all the variations and unique circumstances that will arise. It is therefore essential that OJD builds in adequate flexibility to permit staff and judges to easily and quickly respond to unique situations.

4. Models Available to Protect Confidentiality

A. Restrict public access by case types

For example, significantly limit public and court staff access to adoption, mental commitment, and juvenile cases.

B. Restrict public access by user type

- Public View
- Basic Subscription View
- OSB/Authorized Users View[i]
- Party/Attorney of Record View
- Limited Party View
- View by Court Order Only

C. Restrict access by document type

- Do not provide public access to specific types of documents that have little or no public value but contain confidential information (such as, possibly, returns of service, notices of default, writs of garnishment). Rules would have to require standard labels on such documents. How well confidential information in such documents would be protected would depend on the level of party compliance and court staff's ability to recognize such documents and act accordingly.
- Require or provide the opportunity to file full versions and redacted versions of documents. Parties, judges, and court staff would have access to the full versions; the public would have access only to the redacted version. (This approach is the most labor intensive for both parties and court staff, but would be most useful respecting such documents as a motion for summary judgment or a letter opinion, where references to confidential information is dispersed through-out the document and not easily isolated).
- Require or provide the opportunity to put confidential information on a separate page, such that the primary part of the document would be available to the public and the separate page would not. (This approach would be most useful respecting documents such as some domestic relations filings that routinely contained specified and easily isolated confidential information. Might also be useful for small claims and FED complaints as to addresses of residential premises and other confidential information.)

- Where appropriate, use of case captions that replace natural persons' names with initials (or any other convention that disguises the true names of natural persons) and perhaps even partial case numbers. (This approach would be useful to allow public access to letter opinions, orders, and judgments in otherwise confidential cases.)

D. Restrict access at the data element level

This tool is not yet available, because it depends on the availability of eFiling using fill-in-the-blank fields. With fill-in-the-blank fields, the ECM system can be programmed to limit access to information in particular fields.

SECTION II. PROPOSED USER ACCESS RECOMMENDATIONS

Law and Policy Confidential Information Work Group Recommendations -- User Access to Electronic Court Documents via the Internet

The Oregon Judicial Department is developing policies, operational rules, and procedures governing the information and electronic documents that will be available for access through the Internet. The type and extent of access will be determined by a combination of the information or documents sought and a person's or company's status. The attached matrix is one step in that process.

The policies, rules, and procedures being developed apply to only Internet access to electronic documents and case records. Existing laws governing access will continue to apply to the paper-based files currently maintained and to any electronic files maintained at and viewed in courthouses.

The Matrix Described

The matrix divides documents into six categories and users into five categories. The document categories broadly distinguish documents that are unsealed and not segregated in nonconfidential cases from those in cases that are segregated under court rule, confidential by law or sealed by the court, regardless of whether a case type is confidential or nonconfidential. Within these two broad categories, users then are categorized by the level and type of access allowed to case documents. Users range from those seeking only basic case-schedule information or wishing to make a payment, to public subscribers who wish to examine documents in various publicly available cases, to lawyers and self-represented parties who are the only users allowed access to certain documents or files in their own case(s) because a document is confidential or the case type is a confidential case type. The matrix also acknowledges access by judges and Judicial Department staff.

The matrix captures the basic approach for assessing who has access to which documents for purposes of OJD's Enterprise Content Management (ECM) system. Future refinements will occur as the Confidential Information Work Group continues to identify confidential data elements (e.g., Social Security numbers, driver license numbers) and types of documents for each case type that should be withheld from Internet posting.

Regarding business and governmental users of case-based information such as collection agencies, title companies, DOJ, CJC, DHS, OSP and DOC ("OSB/Authorized Users"), the matrix is not intended to change their current access to OJIN. For the new ECM system, the matrix allows OJD to develop rules to limit their access to case files or documents in which such users are parties or otherwise are permitted by law to inspect the identified case files or documents, including under the State Court Administrator's authority to grant access under ORS 7.132.

Policy Issue

Stakeholder input is important to refine the matrix, if needed, before programming for the ECM system is finished and public access is available. The Work Group is particularly interested in your views about the access category, "OSB/OSB/Authorized Users View."

The policy debate comes down to whether all public users should have full remote electronic access to all files in nonconfidential cases or only parties to a case and their lawyers should have full remote access. The OSB/Authorized Users View category is a middle ground between these two positions in that it grants full access with some conditions to some users but not to all:

- Some attorneys and parties oppose giving remote electronic access to every document in a domestic relations case or a sexual assault criminal case and support limiting remote access to the parties and their lawyers.

- Others oppose limiting access to unsealed and unsegregated documents in all nonconfidential cases for two reasons:

    1. Unless active OSB members have broad access to all nonconfidential case files and documents, many attorneys will not be interested in subscribing to the ECM system, thus reducing materially the benefits of the system for both the courts and the public.

    2. Remote electronic access should be provided to the same extent as exists with paper files today for any person who goes into a courthouse.

The LPC Confidential Information Work Group believes that, at the document level, the ECM system should allow remote electronic access in the "basic subscription view" in nonconfidential cases to unsealed and unsegregated court orders and judgments, but that access to other documents may vary by case type. Substantive law subgroups are working to identify those documents, if any for a particular case type, over the next few months. Their work will be completed within the framework of this access matrix and basic rules that are being developed separately for redaction of confidential or sensitive information within documents. These redaction rules will be circulated for comment separately.

The middle ground represented by the OSB/Authorized Users View category seeks to provide access to those unsealed and unsegregated documents in nonconfidential cases to OSB and authorized governmental and business users that have a recognizable and legitimate business reason to access information that otherwise is deemed to be confidential. For example, collection agencies and title companies need to confirm that the person named in one case is the person in another case with whom they are dealing in a business matter. These entities will be required by law or by contract to maintain as confidential any information to which they are given remote electronic access. The legislature has authorized a similar approach by statute for access to personal information in DMV records.

An illustration may help. For example, in a dissolution of marriage action, a "Basic Subscription View" user would see the case register and the court's orders and judgments, but not all pleadings, motions, and affidavits. For that same case, a registered "OSB/Authorized Users View" user would see every document in that action—and any other cases the user desires—unless the individual document has been segregated by court rule or sealed by court order. This differentiation protects parties' sensitive information from unlimited remote access while allowing remote electronic access by OSB members and other authorized users who are bound by law or contract to keep the information confidential. This category of user does not limit access to nonconfidential orders and judgments that affect community well being and general commerce. It does, however, deny self-represented litigants the same level of access as members of the OSB.

The majority view within the Law and Policy Work Group and most other state court systems that have grappled with this issue support adopting an OSB/Authorized Users view for several reasons:

1. Once information is released through the Internet via remote access, it cannot effectively be retrieved. Therefore, courts have tended to take a conservative approach to the information that can be accessed remotely, with the understanding that remote access can be expanded at a later date, if desired. This caution argues against starting with everyone having the same level of access to documents remotely that they may have when they walk into a courthouse.

2. Lawyers and some governmental and business users currently are given access to records in OJIN that is not generally available. This category continues that practice as to electronic documents but assures safeguards for sensitive information.

3. Self-represented litigants come to court with some inherent disadvantages that the judicial system cannot and should not try to overcome. Not having remote electronic access to documents in all nonconfidential cases—but retaining access to paper documents and files in all nonconfidential cases in the courthouse—is one of the consequences of self-representation.

4. The increase in identify theft and the significant risk of increased identity theft if self-represented parties or the general public had the same access to case documents as OSB members and authorized users argues against granting everyone access that equals the access of those in this category.

5. Lawyers and the self-represented both would be subject to denial of access if they violate the terms of their subscription by using information inappropriately, but the consequences of being denied access would be much greater for attorneys and other authorized users than for the self-represented or a member of the public. If a member of the public, including a self-represented litigant, were to roam through a number of files to

obtain identity information, denying access after that single broad search is no deterrent, because the damage already will have been done. OSB members and other authorized users are less likely to abuse their access privilege, because they have continuing business needs for access.

No member of the Law and Policy Work Group argues that everyone should have remote electronic access equivalent to that which would be available to those in the OSB/Authorized Users View category. Some argue, however, that self-represented litigants should have the same level of access as members of the Bar. If members of the Bar could benefit in preparing their cases by checking all other cases involving a party or witness, so could a self-represented litigant. Remote electronic access to case records is akin to access to a public law library; nobody advocates giving lawyers access to law library facilities to which self-represented litigants would not have access. The legislative requirement that the Judicial Department make legal forms available to self-represented litigants illustrates a policy decision to help level the field between those represented by attorneys and those who self-represent. The legislature has not accepted that the self-represented must accept inherent disadvantages. Limiting self-represented litigants' remote electronic access while granting attorneys full access to all files, it is suggested, may not withstand legal challenges.

The Law and Policy Work Group is particularly interested in comments concerning the access category of "OSB/Authorized Users View."

USER ACCESS TO DOCUMENTS THROUGH OJD'S E-COURT ECM SYSTEM

The following definitions apply to the column headings on the User Access Matrix. "Confidential Cases" refers to juvenile cases (any type), adoption cases, and mental commitment proceedings.

Public View

- Any User (Free; subscription not required)
- Limited view of next scheduled action in a case and payment information re: fines/fees

NOTE: Access to the following categories will require a paid subscription

Basic Subscription View

- Any User (with subscription)
- Documents in nonconfidential cases only
- Access to most, but not all, documents that have not been sealed or segregated (Subgroups of the LPWG are in the process of determining which documents, in which types of cases, might be excluded from this view.)

OSB/Authorized Users View (2 components)

Component #1 (access provided following execution of agreement to maintain confidentiality)

- Active OSB Members/Other Authorized Users (with subscription)
- Documents in nonconfidential cases only
- Unrestricted access to all case files and documents that have not been sealed or segregated

Component #2:

- Non-Represented Parties/Pro Hoc Vice Lawyer Users (with subscription)
- Documents in nonconfidential cases only
- Access to all documents that have not been sealed or segregated, in own cases only (for pro hoc vice users, cases in which admitted as counsel of record)

Party/Attorney of Record View

- Parties/Active OSB Members/Pro Hoc Vice Lawyer Users (with subscription)
- Documents in confidential cases
- Access to all documents in own cases only, except documents that have been sealed or segregated as to which the party and the party's lawyer have no right to access

Limited Party View

- Parties/Active OSB Members/Pro Hoc Vice Lawyer Users (with subscription)
- Sealed or segregated documents in nonconfidential and confidential cases
- Access to own sealed or segregated documents, in own cases only

View by Court Order Only

- For case types that are confidential by law (e.g., adoption, mental health) and for certain documents that are sealed by law or by court order, access is available only by operation of law or by court order

USER ACCESS MATRIX

	Unsealed/Unsegregated Documents in Nonconfidential Cases			Documents in Confidential Cases and Sealed/Segregated Documents in Other Cases		
User Type	Public View	Basic Subscription View	OSB/Authorized Users View*	Party/Attorney of Record View	Limited Party View	View by Court Order Only -- sealed & closed docs or when law changes classification based on an event (e.g., arbitration award)
Basic – limited case register fields	X					
Subscription— General User Public Access	X	X				
Subscription— OSB Member Protected Access	X	X	X			
Subscription— Party and Lawyer Case Access	X	X	X	X		
Subscription— Party and Lawyer Document Access	X	X	X	X	X	

- This view distinguishes active OSB from non-OSB (pro hac vice/specially admitted from out of state) lawyers

	Unsealed/Unsegregated Documents in Nonconfidential Cases			Documents in Confidential Cases and Sealed/Segregated Documents in Other Cases		
User Type	Public View	Basic Subscription View	OSB/Authorized Users View*	Party/Attorney of Record View	Limited Party View	View by Court Order Only -- sealed & closed
General OJD Access	X	X	X			
Confidential OJD – statewide • All • By case type	X X	X X	X X	X By case type	X By case type?	
Confidential OJD – own court only	X	X	X	X	X	
Confidential OJD – own court only; limited case types	X	X	X	By case type	By case type	
Some very limited personnel • Statewide-all • Statewide by case type • Own Court – all • Own Court – by case type	X X X X	X X X X	X X X X	X By case type X By case type	X By case type X By case type	X By case type X By case type

SECTION III. REDACTION-SEGREGATION SUBGROUP RECOMMENDATIONS

July 7, 2009

MEMORANDUM

To: Confidential Information Workgroup
Fr: Redaction Segregation Subgroup
Re: Confidentiality Recommendations

I. OVERVIEW OF THE REDACTION SEGREGATION SUBGROUP

The Confidential Information Workgroup formed the Redaction Segregation Subgroup (the "Subgroup") to develop recommendations addressing public electronic access to filings with the courts. Members of the Redaction Segregation Subgroup include:

- Joel Bruhn, Legal Analyst, CPSD
- Nori Cross, Special Counsel, Executive Services
- Brian DeMarco, Staff Counsel, CPSD (Chair)
- Bruce Lowther, ECM Systems Analyst
- Jim Nass, Appellate Commissioner, Appellate Court Services
- Lorraine Odell, Information Security Officer, BFSD
- Rebecca Orf, Juvenile Law staff counsel, CPSD
- Erin Ruff, Analyst, CPSD (Staff)
- Robin Selig, SFLAC Representative
- Brenda Wilson, Court Records and Procedures Analyst

The Redaction-Segregation Subgroup was charged with determining (1) what information should be protected in all case types, and (2) mechanism(s) for protection of information in all case types. In addition, case-type committees (i.e., civil, criminal) were formed and charged to review and comment on the Redaction Segregation Subgroup's draft recommendations. This memorandum includes those reviews and the Subgroup's resulting recommendations.

II. RECOMMENDATIONS ON PUBLIC ELECTRONIC ACCESS TO COURT FILINGS.

A. DEVELOP AND ADOPT COURT RULE(S)[1] TO DIRECT AND GOVERN ELECTRONIC ACCESS.

The gradual roll-out of Oregon eCourt by judicial district and case type, and the ongoing co-existence of conventional and eFiling, will require that such rules also take into account that many documents will continue to be filed conventionally, and that documents will continue to be

[1] The Subgroup has been working on a draft UTCR, tentatively numbered UTCR 2.112. However, the draft rule is long, with many subsections, and the Subgroup is considering breaking it down into multiple smaller rules and making them part of a new chapter 22 of the UTCR (following the new UTCR chapter of rules on eFiling). Also, note that the Subgroup will likely be recommending that the appellate courts and the Tax Court, by rules(s), adopt comparable provisions.

made available at the courthouse conventionally. Because many documents will continue to be filed conventionally and courts will need to make some documents available conventionally at the courthouse, Oregon eCourt will require the rules take into account paper documents.

The court rule regarding electronic content management would become effective in a local court when the State Court Administrator "acknowledges" that court's electronic content management system. The Subgroup recommends that the court rule contain provisions addressing the following:

1. Define personal and sensitive information to protect in all case types;
2. Place the burden of protecting personal and sensitive information contained in party-created documents on the parties, and on the court for court-created documents;
3. Define filings and documents subject to restricted online access;
4. Create a process to delay online access to filed documents (except to named parties and attorneys of record) to allow time for objections based on inclusion of protectable personal and sensitive information;
5. Create a process to handle objections to information included in or redacted from a filing; and
6. Make available three (3) mechanisms to protect information as appropriate in each individual case types – redaction, segregation and sealing.

B. ADOPT ONE STANDARD LIST OF SENSITIVE INFORMATION TO PROTECT IN BOTH CONVENTIONAL AND ONLINE ENVIRONMENTS BY:

1. Revising UTCR 2.100 as recommended in Exhibit A;
2. Amending ORAP 8.50; and
3. Adopting court rules that reference UTCR 2.100 as revised

The following personal and sensitive information across all case types should be protectable from online disclosure; this information is or will be covered under current UTCR 2.100:

<u>Identifying Information:</u>

- Former names;
- Full birth dates;
- Places of birth;
- Full Social security numbers;
- Full driver license or other state-issued identification numbers;
- Full passport or other United States-issued identification numbers; and
- Names of minors

<u>Contact Information:</u>

- Of certain victims and witnesses; or
- That is confidential or exempt from disclosure by state or federal law or court order

<u>Financial Information:</u>

- Bank or other financial account locations;
- Full Credit card numbers;
- Full bank or other financial account numbers;
- Financial account access codes; or
- Similar information that is used for financial transactions and can be kept confidential by state or federal law or court order

<u>Other Information:</u>

- Information that is exempt from public inspection under state or federal law or court order

C. REVIEW AND RECONCILE COURT RULES THAT INCLUDE DEFINITIONS RELEVANT TO ELECTRONIC CASE MANAGEMENT.

The definition of "protected personal information" in ORAP 8.50 differs from that in UTCR 2.100. See also how ORAP 1.35(1)(b) treats party contact information, and note that ORAP 16.60 cross-references ORAP 8.50. There are also variations in how rules define protectable personal, residential, employment or mailing information; as opposed to address, phone number and/or email addresses at which the person can be contacted by the court and other parties to the case for notice and service. These are some examples of variations in definitions of important terms that should be addressed and may need to be reconciled. Furthermore, the case-type subgroups may raise issues and suggest definitions for use within the ECM system that may need to be reconciled with definitions elsewhere.

D. RESTRICT ONLINE ACCESS TO ALL DOCUMENTS FILED WITH THE COURT FOR A SPECIFIED NUMBER OF DAYS.

To allow opposing parties a meaningful opportunity to request protection of personal information, the Subgroup recommends:

1. Limiting any document filed to “restricted” or “secure” access during which any person can request protection of personal and sensitive information as defined;
2. Publishing documents according to proposed document access matrix, as revised by the recommendations of the Law and Policy Committee after consideration of the work of each case-type subgroup, only after:
    a. For a case-initiating document: 30 days from the date of service on all parties to the action (or appearance where a party appears before filing of the return of service as to that party); or
    b. For subsequent filings, including court-created documents: 14 days from the date of filing with the court; and
    c. A decision has been made on any requests for protection or publication.
3. Providing a form for requests for protection or publication of personal information via court rule; and
4. Adopting rules to address disputes regarding disclosure of personal or sensitive information.

E. PROGRAM ECM TO AUTOMATICALLY ASSIGN APPROPRIATE ACCESS LEVELS BASED ON FOUR IDENTIFIERS[2]:
   1. Case type (certain case types will be categorically confidential, such as Juvenile, Mental Health and Adoption);
   2. Document type (certain document types will be protected, such as Returns of Service);
   3. Security label on document (such as segregated, redacted or sealed); and
   4. Unique individual identifier of the parties referenced in the document (recognizing that OJD may not be able to implement this recommendation pending development of an individual identification system and modification or replacement of OJIN).

F. RECOGNIZING THAT IN SOME INSTANCES A PERSON TENDERING A DOCUMENT FOR FILING AS A PROTECTED DOCUMENT MAY FAIL TO LABEL THE DOCUMENT PROPERLY, BY RULE OR POLICY THE OJD SHOULD ALLOW BUT NOT REQUIRE COURTS TO GIVE THE PERSON WRITTEN NOTICE:
   1. To correct the document within a specified period of time; and
   2. That if the person fails to correct the filing in that time, the document may become available to the public on the Internet.

   **THIS RECOMMENDATION DOES NOT APPLY TO DOCUMENTS THAT THE COURT PROPERLY REJECTS UNDER STATUTE OR RULE.

The subgroup preferred this alternative to one that would allow the court to dismiss a pleading or deny a motion, believing that the recommendation requires less staff work and no judge involvement. The recommendation does not require courts to send notice, but presumes that courts can classify many or most documents even if they do not comply with whatever identifiers a new UTCR may require filers to include. The recommendation keeps the burden on the filers and parties to the case to ensure that they provide the information the court needs to protect protectable information, consistent with the Confidential Information Workgroup's Foundational Principles. ECM should include a field to enter that the court has sent a notice to correct by a certain date and either tickle the document for review within 10 days to determine whether the court has received a correction (as courts review for return of service) or to publish within 10 days if no correction is entered. If the court receives correction in meantime, clerk can cancel the auto schedule and edit as needed.

Because state law provides very limited authority to reject filings and because the subgroup believes that self-represented litigants will find this process complex and make mistakes, the recommendation avoids additional work of dismissing pleadings/cases or denying motions for failure to comply; instead the sanction for failure to comply is that the document is public unless it is in a categorically confidential case.

[2] Document access rules based on these four identifiers are being developed.

G. LIMIT DISCLOSURE OF CONTACT ADDRESSES OF NATURAL PERSONS, AS MUCH AS PRACTICABLE, TO USERS WHO HAVE A LEGITIMATE BUSINESS INTEREST IN THE INFORMATION **AND ARE OBLIGATED BY LAW OR CONTRACT** NOT TO REDISCLOSE THE INFORMATION.

The Subgroup recommends that court rules define "contact address" to include residential or mailing addresses, not including "alternate" contact addresses provided under statute or rule.

The Subgroup also recommends that the courts:

1. Stop disclosing contact addresses and other personal identifying information contained in non-civil cases through OJIN to the general public (i.e. criminal, traffic, violations, etc). For these purposes, “general public” should be differentiated from stakeholders with a legitimate business purpose, including but not limited to bulk data customers, law enforcement, and other similar agencies;
2. Limit online access to contact information contained in ECM data fields to the “restricted” or "secure" view;
3. Limit online access to scanned citations that contain address information (such as traffic, boating, and game violations) to the “restricted” or "secure" view until such time as the uniform statewide citations are revised to protect contact addresses and other "protected personal information" as defined by UTCR 2.100 (2)(a); and
4. Adopt a procedure to allow any natural person to cause their contact address, which otherwise would be part of a document filed with the court, to be protected from public disclosure.

H. FOR ANY RECORD (PAPER OR ELECTRONIC) FILED BEFORE THE ACKNOWLEDGMENT OF ECM FOR THAT COURT, GIVE THE LOCAL COURT DISCRETION TO ENTER THOSE DOCUMENTS INTO ECM ON A CASE-BY-CASE BASIS, CLASSIFYING ANY SUCH DOCUMENTS AS “BACKLOADED” WITH ACCESS LIMITED TO JUDICIAL OFFICERS AND COURT STAFF ONLY UNLESS THE COURT GRANTS PARTY ACCESS CASE BY CASE.

I. DEVELOP RULES, FORMS, PUBLIC OUTREACH MATERIALS, POSTERS, SELF-HELP INSTRUCTIONAL MATERIALS TO INFORM ALL PARTIES ABOUT ONLINE PUBLICATION, AND THE OPPORTUNITY AND PROCESS TO REQUEST PROTECTION OF PERSONAL AND SENSITIVE INFORMATION.

SECTION IV. DRAFT UTCR CHAPTER 22

08/03/09.1 Version

CHAPTER 22. ELECTRONIC CONTENT MANAGEMENT SYSTEM

CHAPTER 22. ELECTRONIC CONTENT MANAGEMENT SYSTEM

UTCR 22.010. Purpose; Authority to Waive/Modify.

(1) The Judicial Department is establishing an electronic content management (ECM) system that will maintain ~~court~~ **case** records electronically rather than by paper and that will allow access to those ~~court~~ **case** records via remote electronic access. Making ~~court~~ **case** records available via remote electronic access facilitates public access to ~~court~~ **case** records, and commensurately increases the risk of disclosure of information that is protected by law, that can be used in identify theft and financial fraud, that can identify children who are involuntarily parties to or the subject of legal proceedings, and that can place at risk the personal safety and liberty of some persons. The purpose of this rule is to establish procedures for persons and the court to facilitate reasonable access to electronically-maintained ~~court~~ **case** records via remote electronic access and, at the same time, avoid inappropriate disclosure of protected information in those records.

(2) The primary responsibility for avoiding inappropriate disclosure of protected information rests with the person filing a document. A person who believes that protected information about that person may be or has been disclosed is responsible for using the procedure provided in these rules to challenge the disclosure. The trial court administrator should encourage compliance with these rules, but need not review each filed document for compliance and should not reject for filing any non-compliant document.

(3) The court on its own motion or on the motion of any person may waive or modify any provision of this chapter as necessary or convenient to achieve the purpose of this chapter.

UTCR 22.020. Effective Dates; Applicability.

(1)(a) The electronic content management system initially will be operational only in certain judicial districts and for certain types of cases, but eventually will be operational in all judicial districts and all case types. As the electronic content management system becomes operational in one or more judicial districts and for one or more specific case types, the State Court Administrator will certify those facts, together with the date that the system becomes operational for those cases. The State Court Administrator's certifications will be published online at *[specify OJD web location where this information or a link to the information will be published]*.

(b) This rule is applicable only to a case filed in the judicial district and in a case type certified by the State Court Administrator as ready to be maintained in electronic form, on or after the date specified in the State Court Administrator's certification. A court may make documents filed before the State Court Administrator's certification date part of the electronic content management system, but the documents will be available only to the court and its personnel**, to the parties as determined by the court on a case by case basis,** and will not be available ~~to parties or~~ the public via remote electronic access.

(c) Notwithstanding that the electronic content management system becomes operational in a judicial district and for specified case types, the court will continue to make ~~court~~ **case** records available at the courthouse as if the records were maintained in paper form, such as by providing a computer terminal for 20viewing case records maintained in electronic

form and by providing paper copies on request.

UTCR 22.030. Definitions Generally.

As used in this chapter:

(1) "Attorney" means the attorney of record in a case.

(2) "Case" means an action or proceeding.

(3) "Case record" means the court file as provided in ORS 7.095, excluding exhibits and the record of oral proceedings of the court.

(4) "Court contact information" means the name, mailing address, telephone number and fax number, if any, , as to a person whose personal contact information is not subject to disclosure, alternative contact information sufficient to enable the court to communicate with the person and to enable any other party to the case to serve the person under UTCR 2.080(1).

(5) "Document" has the same meaning as provided in UTCR 21.010(2).

(6) "Initiating document" means a complaint, petition, indictment, information, or other document that initiates a case, and a cross-complaint, cross-petition, or other document that adds a person as a party to case.

(7) "Remote electronic access" means access to **case** records ~~of court cases~~ in the Oregon Judicial Information Network (OJIN), including the electronic content management system, via the Internet.

(8) "Secure case" means:

(i) An adoption case subject to ORS 7.211, a juvenile court case subject to ORS 419A.255 and ORS 419A.256, a mental commitment case subject to ORS 426.160 or ORS 427.293, *[a domestic relations case subject to UTCR chapter 8?]*, ~~and~~ [*the record of a case initiated by the filing of an arbitration award under ORS _____ until the court enters judgment on the award,?*] **, and a drug court program case subject to ORS 3.450,** and

(ii) Consistent with the limitations on disclosure of information in case records imposed by 18 USC § 2265(3), ~~the case record in~~ the following case types: Family Abuse and Prevention Act cases, Elderly Persons and Persons With Disability Abuse Prevention Act cases, **and** civil stalking protective order cases pursuant to ORS 30.866 or ORS 163.738*[~~, and any other case in which a person is seeking a protection or restraining order for the personal safety or liberty of the person or the person's minor children~~ to be determined?].*

UTCR 22.040. When Documents Become Available Via Internet.

(1)The court will not make any document filed with a court available via remote electronic access until after expiration of:

(a) Thirty days following the date of filing of proof of service of the initiating document on the defendant or, if there is more than one defendant, the filing of proof of service of the initiating document on all defendants or following the appearance by ~~a party~~ **all defendants,** whichever is earlier**, or a combination of proof of service on or appearance by all**

defendants. Upon motion of a party and for good cause shown, the court may direct that any document filed in a case in which there are multiple parties be made available via remote electronic access notwithstanding that the party filing the document has not provided proof of service on all other parties to the case or that not all parties have appeared.

(b) Fourteen days following the date of filing of any document other than an initiating document.

(2) During the time periods prescribed in subsection (1) of this rule**,** if a party seeks relief under UTCR 22.110, the trial court administrator will not make the document available via remote electronic access until the request has been resolved.

(3) When a person files an initiating document in a case type in which the documents may be available via remote electronic access, the person must accompany the initiating document with a notice in the form prescribed in UTCR Form 22.040.3. informing any other party to the case that documents filed in the case may be available via remote electronic access, the opportunity of the person to seek relief under UTCR 22.110 and the time within which the request for relief must be filed. When a party files a cross-complaint, cross-petition, or other document that adds a person to the case, the party must provide the notice prescribed in this clause only to any person being added as a party to the case

UTCR 22.050. Definition of Protected Information.

As used in this rule, "protected information" means:

(1) Protected personal information as defined in UTCR 2.100(2)(a) and (b).

(2) Personal contact information of a natural person.

(a) "Personal contact information" means the residential address, mailing address (if different from residential address), any telephone number, facsimile transmission number, email address, Internet Protocol address, or other similar means by which a natural person may be contacted personally and directly.

(b) "Personal contact information" excludes court contact information**, and excludes** contact information about a person's place of employment unless the person is the victim or a witness, other than a law enforcement officer in the capacity of a law enforcement officer, in:

(i) A criminal or juvenile delinquency case; or

(ii) A Family Abuse and Prevention Act, Elderly Persons and Persons With Disability Abuse Prevention Act, civil stalking order pursuant to ORS 30.866 or ORS 163.738, and any other case in which a person is seeking a protection or restraining order for the personal safety or liberty of the person or the person's minor children.

(3) The name of a person under the age of 18 years who is not voluntarily a party to or the subject of a legal proceeding.

(4) Any photograph of involuntary nudity **of a natural person**, obscene materials, **or other explicitly sexual material,** and any photograph of a victim of crime.

(5) Information that can be made confidential under ORS 25.020(8)(d), ORS 109.767(5), ORS 110.375, or ORS 192.445 or 22that otherwise is exempt from public

inspection under state or federal law.

(6) Information protected by other specific law or by court order.

UTCR 22.060. Avoiding Disclosure of Protected Information.

(1) Subsections (2), (3), and (4) of this rule prescribe the means available in this chapter to avoid inappropriate disclosure of protected information in documents filed with the court. A person filing a document containing protected information *about another person must* use one of the prescribed means. Except as provided in subsections (5) and (6) of this rule, a person filing a document containing protected information *about the person may* use one of the prescribed means.

(2) Segregated Documents.

(a) Segregation means that protected information is set forth on one or more pages separate from the primary document. The primary document must be labeled "Segregated Document" and the separate page must be labeled "Segregated Information." "Page" includes pages if the segregated information consists of multiple pages. A party may refer to protected information by referring to a party by that party's status (for example, child, husband, wife, mother, father, personal representative), by use of an assumed name or initials, by truncating numbers, or by any other suitable convention that maintains the readability of the primary document and avoids disclosure of protected information**.** A party may file segregated information also labeled as "Sealed" as provided in ~~paragraph (3)(b)~~ **subsection (5)** this rule.

(b) If a person files protected information by a segregated document, as long as the specific protected information remains current, a person need not re-submit the protected information each subsequent time that the already segregated information otherwise would be submitted in that case. The person should add a written notation to any document subsequently submitted to the effect that the information already has been submitted in the case under this rule.

(c) A document filed under UTCR 2.100 or UTCR 2.110 must be filed as a segregated document.

(3) Confidential Documents.

(a) A confidential document is a document that, by law or court order, is available to other parties to the case but is not available to the public. If a document is not protected from disclosure by law, a party seeking to prevent access to the document via remote electronic access must file a motion seeking a protective order. A confidential document must be labeled "Confidential Document Under _____" and identify the law or court order under which the document is confidential.

(b) The following documents must be filed as confidential documents:

(i) Any report or similar document submitted directly to a court by a social worker, licensed medical or mental health practitioner, presentence investigator, or other similar person, which report contains alcohol or drug, mental or medical information about a person or otherwise contains information that is not subject to public disclosure, including but limited to a court visitor's report in a protective proceeding under ORS Chapter 125, a child custody study, a presentence investigation report, and a report concerning a defendant's fitness to proceed or

criminal responsibility under ORS Chapter 161.

(ii) Any photograph of involuntary nudity **of a natural person**, obscene materials, **or other sexually explicit material,** or [~~a~~] **any** photograph of a crime victim;

(iii) An affidavit or declaration in support of a motion to waive or defer court costs and fees under ORS 21.605.

(iv) Any return of service, if the return of service contains personal contact information of the person served.

(v) Any list of assets or other document in a probate, domestic relations, or other type of case that includes financial information as defined in UTCR 2.100(2)(b)(i).

(vi) Any confidential information form filed under UTCR 2.130 **that is not filed as a sealed document**.

(4) Redacted Documents. Redaction means that the person submits two ~~copies~~ **versions** of ~~the~~ **a** document~~,~~**:** a complete version with no content hidden from view**,** and a redacted version with protected information hidden from view. The complete version ~~of the document~~ must be labeled "Complete Version of Redacted Document" and the redacted version must be labeled "Redacted Version Document." Parties are encouraged to use redaction only when filing a segregated or confidential document is not practical or appropriate under the circumstances.

(5) Sealed Documents. A sealed document is a document that, by law or court order, is not available for viewing by any other party to the case or by the public. A party may file a sealed document only upon order of the court. A sealed document must be labeled "Sealed Document Under _____" and identify the **law or** court order under which the document is sealed.

UTCR 22.070. Service of Documents Containing Protected Information.

For purposes of UTCR 2.080(1), a person filing a document subject to this chapter must mail or deliver to parties the segregated document and the page of a document containing segregated information, a confidential document, and the complete version and the redacted version of a redacted document unless the person, based on specific legal authority, believes that the person is entitled to prevent disclosure of the protected information in the document to that party. If a person serves less than a full copy of a document on a party, the certificate of service accompanying the document shall describe the document or part of a document that was not served on the party.

UTCR 22.080. Court Response to Documents Filed Under This Chapter.

Generally and subject to the provisions of UTCR 22.100 and 22.110, when a segregated, confidential, redacted**,** or sealed document is filed under this rule, the trial court administrator will restrict access to the document or part of the document containing protected information as follows:

(1) The primary document of a segregated document will be made available to the public via remote electronic access, but the segregated page will not and will be made available only to the parties to the case, unless the segregated page was filed as "Sealed," in

which case the document will only be available to the court.

(2)(a) A document labeled "Confidential" will not be available to the public via remote electronic access, but will be made available to the parties.

(b) A document labeled "Sealed" will not be made available to either the public or to any party, except with leave of the court.

(3) The parties to a case will have access via remote electronic access to the complete and redacted versions of a redacted document, but the public will have access via remote electronic access only to the redacted version of a document.

UTCR 22.090. Protected Information in Court-Generated Documents.

The court is responsible in the first instance to insure that any notice, letter opinion, order, judgment or other writing issued by the court does not make protected information available via remote electronic access to a person not entitled under this rule to access the information. A person adversely affected by an inappropriate disclosure may file a request with the court to take measures as necessary to avoid the inappropriate disclosure. A person seeking relief under this paragraph may use the form substantially like UTCR Form 22.090 to present the request. The trial court administrator will resolve the request, subject to review by the court on motion of a person adversely affected by the trial court administrator's resolution.

UTCR 22.100. Viewing Case Records Via Remote Electronic Access

(1) Basic Public View. With respect to a case other than a secure case, any person, without a subscription to OJIN, may view via remote electronic access the full case title, the case number, the next scheduled event in the case, if any, and, if the court has imposed a fine or a fee, the amount of the fine and fee owing at that time.

(2) Expanded Subscription Public View. Any person who has subscribed to OJIN may view via remote electronic access the **case** record of any case except**:**

(a) In a secure case, the entire case record;

(b) In case other than a secure case, the segregated page of a segregated document, a confidential or sealed document, and the unredacted version of a redacted document.

(3) Party/Attorney View. Any party to a case or any attorney for a party, including an attorney admitted *pro hac* vice, who has subscribed to OJIN may view via remote electronic ~~access all documents in~~ the case **record** except, in a secure case:

(a) Any sealed document, and

(b) In an adoption case subject to ORS 7.211, ~~no party or attorney for a party may view~~ **any part of** the case record after entry of the general judgment of adoption.

(4) In a ~~confidential~~ **secure** case, ~~the parties, but not~~ the public~~,~~ may **not** have access to the **case** record via remote electronic access.

(5) If the court sets aside a conviction under ORS 137.225 or orders expunction of a case record under ORS 419A.260 and 419A.262, neither the public nor the parties ~~will~~ **may** have access to the case record via remote electronic access.

(6) State court judges and Judicial Department personnel may view the **case** record of any case via the ECM system as necessary and convenient to carry out the duties of the court and the Department**, *[except that a judge may not view an arbitration award to the extent provided under ORS _____?]***.

[(7)(a) An attorney representing a party in a domestic relations case may apply to the Judicial Department for access to the records of domestic relations cases. Any attorney having access to the record in a domestic relations case shall maintain as confidential information derived from the record of a domestic relations case.?]

(b) Any government agency or business entity for whom it is necessary and convenient for the business purpose of the agency or business **may apply to the Judicial Department for access as appropriate via the ECM system** ~~as appropriate to have access~~ to the **case** record~~s~~ of ~~confidential cases~~ **a secure case, except for any sealed document in the case,** or the segregated page of a segregated document~~,~~ **or** the full version of a redacted document~~, or sealed documents~~ in **a** non-~~confidential~~**secure** case~~s may apply to the Judicial Department for access to such records or documents via the ECM system as appropriate~~. The Judicial Department will grant access to such cases or documents as appropriate for the agency's business purpose. Any agency or business entity having access to protected information shall maintain the information as confidential.

UTCR 22.110. Confidentiality Motions and Determinations.

(1) Where protected information about a person in a document filed with a court has not been adequately protected from disclosure, the trial court administrator, on the trial court administrator's own initiative or at the request of a person adversely affected by the disclosure, may require the person who filed the document to refile it in a manner that avoids disclosure of protected information or may restrict access to the document consistent with this rule. A person seeking relief under this paragraph may use the form substantially like UTCR Form 2.110.1 to present the request**.** A person adversely affected by the trial court administrator's resolution may request review of the trial court administrator's decision. The request must be in the form of a motion filed in the manner prescribed by UTCR 5.020 to 5.050.

(2) If the court, on motion of a person or on the court's own motion after giving the person filing a document reasonable notice and opportunity to be heard, determines that a document filed under this rule does not contain protected information or, if the document contains protected information but was filed in a manner that restricts access to the document via remote electronic access inconsistent with this rule, the court may direct the trial court administrator to modify, as appropriate, access to the document via the remote electronic access system. A person seeking relief under this paragraph may use the form substantially like UTCR Form 22.100.2 to present the motion.

UTCR 22.120. Exhibits.

The court may scan documentary exhibits offered and received by the court or offered as an offer of proof, and make such exhibits ~~part of the record of the case in~~ **available via** the electronic content management system. The court may arrange with the parties to submit documentary exhibits in digital form, provided that the form of submission allows the exhibits to become part of the electronic content management system. The parties to the case, but not the public, will have access to the exhibits via remote electronic access.

UTCR 22.130. Record of Oral Proceedings.

(1) When the electronic content management system acquires the capability to capture audio and visual recordings of proceedings before the court, the audio or visual records will be available to the parties to the case, but not the public, via remote electronic access.

(2) If prepared and filed with the court, the transcript of a proceeding before the court will be maintained as part of the electronic content management system and will be available to the parties and**, except in secure cases, to** the public via remote electronic access.

Definitions in Existing UTCR

UTCR 1.110 Definitions

As used in these rules:

(1) Party means a litigant or the litigant's attorney.

(2) Trial Court Administrator means the court administrator, the administrative officer of the records section of the court, and where appropriate, means trial court clerk.

(3) Plaintiff and Petitioner mean any party asserting a claim for relief, whether by way of claim, third-party claim, crossclaim, or counterclaim.

(4) Defendant and Respondent mean any person against whom a claim for relief is asserted.

(5) Days mean calendar days, unless otherwise specified in these rules.

UTCR 21.010 Definitions

The following definitions apply to this chapter:

(1) "Conventional filing" means a process where a filer files a paper document with the court.

(2) "Document" means a pleading, a paper, a motion, a declaration, an application, a request, a brief, a memorandum of law, an exhibit, or other instrument submitted by a filer, including any exhibit or attachment referenced in the instrument. Depending on the context, as used in this chapter, "document" may refer to an instrument in either paper or electronic form.

(3) "Electronic filing" means the process where a filer electronically transmits to a court a document in an electronic form to commence an action or to be included in the court files for an action.

(4) "Electronic filing system" means the system provided by the Oregon Judicial Department for the electronic filing and the electronic service of a document via the Internet. A filer may access the system through the Oregon Judicial Department's website (http://www.ojd.state.or.us).

(5) "Electronic service" means the electronic transmission of a notice of filing or a notice of a scheduled court proceeding by the electronic filing system to the electronic mail (e-mail) address of a party registered as a filer with the electronic filing system. The notice may contain a hyperlink to access a document that is filed electronically for the purpose of effecting service.

(6) "Filer" means a person registered with the electronic filing system who submits a document for filing with the court.

(7) "Pro se litigant" means a person who by law may appear in an action without a lawyer.

[i] OSB/Authorized Users View may include members of the Bar who are not the attorney of record, self-represented parties, and identified commercial interests.